Secure*BPMN - a graphical extension for BPMN 2.0 based on a Reference Model of Information Assurance & Security

A thesis submitted in partial fulfilment

of the requirement for the degree of Doctor of Philosophy

Yulia Cherdantseva

December 2014

Cardiff University
School of Computer Science & Informatics

Declaration

This work has not been submitted in substance for any other degree or award at this or any other university or place of learning, nor is being submitted concurrently in candidature for any degree or other award.

Signed . . . . . (candidate) Date . . . . . .

Statement 1

This thesis is being submitted in fulfilment of the requirements for the degree of PhD.

Signed . . . . . (candidate) Date . . . . . .

Statement 2

This thesis is the result of my own independent work/investigation, except where otherwise stated. Other sources are acknowledged by explicit references. The views expressed are my own.

Signed . . . . . (candidate) Date . . . . . .

Statement 3: PREVIOUSLY APPROVED BAR ON ACCESS

I hereby give consent for my thesis, if accepted, to be available online in the University's Open Access repository and for inter-library loans after expiry of a bar on access previously approved by the Academic Standards & Quality Committee.

Signed . . . . . (candidate) Date . . . . . .

To my family

Abstract

The main contribution of this thesis is Secure*BPMN, a graphical security modelling extension for the de-facto industry standard business process modelling language BPMN 2.0.1. Secure*BPMN enables a cognitively effective representation of security concerns in business process models. It facilitates the engagement of experts with different backgrounds, including non-security and non-technical experts, in the discussion of security concerns and in security decision-making. The strength and novelty of Secure*BPMN lie in its comprehensive semantics based on a Reference Model of Information Assurance & Security (RMIAS) and in its cognitively effective syntax.

The RMIAS, which was developed in this project, is a synthesis of the existing knowledge of the Information Assurance & Security domain. The RMIAS helps to build an agreed-upon understanding of Information Assurance & Security, which experts with different backgrounds require before they may proceed with the discussion of security issues. The development process of the RMIAS, which was made explicit, and the multiphase evaluation carried out confirmed the completeness and accuracy of the RMIAS, and its suitability as a foundation for the semantics of Secure*BPMN. The RMIAS, which has multiple implications for research, education and practice is a secondary contribution of this thesis, and is a contribution to the Information Assurance & Security domain in its own right.

The syntax of Secure*BPMN complies with the BPMN extensibility rules and with the scientific principles of cognitively effective notation design. The analytical and empirical evaluations corroborated the ontological completeness, cognitive effectiveness, ease of use and usefulness of Secure*BPMN. It was verified that Secure*BPMN has a potential to be adopted in practice.

Acknowledgements

I would like to thank my supervisors for their support, guidance and encouragement during my work on this thesis, and for helping to develop my research skills.

I would like to thank sincerely Mr Jeremy Hilton, who supervised me throughout all this research project, for being always available, for long and interesting discussions and for the approach to information security I adopted.

I would like to thank Professor Omer Rana for showing me a different perspective, for challenging my assumptions and for making me stronger in defending my opinion.

I would also like to thank Dr Wendy Ivins for providing insightful comments, for helping to improve the clarity and structure of the thesis tremendously.

I was only able to go through this endeavour because of the continuous support of my husband Mikhail, my parents and children who stood by me throughout the years of my study.

I also thank all colleagues at the School of Computer Science & Informatics, Cardiff University and at other organisations who contributed to the consolidation of my ideas.

Contents

List of Figures

List of Tables

List of Acronyms

BPM Business Process Management

BPMN Business Process Model and Notation

IA Information Assurance

IAS Information Assurance & Security

ICT Information and Communication Technology

InfoSec Information Security

IS Information System

ISDLC Information System Development Life Cycle

ISPD Information Security Policy Documents

IT Information Technology

ItU Intention to Use

MEM Method Evaluation Model

MEMO Multi-perspective Enterprise Modelling

MDA Model-Driven Architecture

MDE Model-Driven Engineering

OMG Object Management Group

PAIS Process-Aware Information Systems

PEOU Perceived Ease of Use

PU Perceived Usefulness

RMIAS Reference Model of Information Assurance & Security

SME Small- and Medium-size Enterprise

SOA Service-Oriented Architecture

TVND Theory for Visual Notation Design

UML Unified Modelling Language

Chapter 1

Introduction

1.1 Research Context

The work presented in this thesis lies in the overlap of two domains - **Information Assurance & Security** (IAS) and **Business Process Management** (BPM). More specifically, this thesis develops and evaluates a modelling technique which allows the representation of IAS-related information in business process models. Specific attention in this research is paid to cross-organisational information sharing which is an inevitable part of cross-organisational business processes.

In the foundation of this research lies an assertion that IAS-related details may be effectively captured within business process models. This assertion is well-founded in the existing literature (Chapter 5). The benefits of representing IAS details in business process models are discussed in Section 1.1.4. Preceding this discussion, first, the importance of IAS, the critical role of business processes in an organisation and the challenges of cross-organisational information sharing are considered in Sections 1.1.1, 1.1.2 and 1.1.3 respectively in order to set the context. Then, the approach to IAS and an Information System adopted in this thesis is explained in Section 1.1.5.

1.1.1 The Importance of Information Assurance & Security (IAS)

IAS has become increasingly important in an era in which information is recognised as a key asset by many organisations. The rapid advancement of Information and Communication Technology (ICT) and the growing dependence of organisations on ICT infrastructure continuously intensify the interest in the domain. Organisations pay increasing attention to information protection also because the impact of security breaches today has a more tangible, often devastating effect on business [1].

The number and severity of security breaches grows. In 2007, TJX Company lost, according to different sources, from 36.2 to 94 million customers' credit and debit cards records [2]. In 2011, Sony reported a data breach that had resulted in the loss of personal details of 77 million customers [3]. The spending on InfoSec worldwide stayed stable in 2011, even despite the economic downturn [4]. In 2012, security budgets received higher priority worldwide compared to 2011 [5]. Gartner predicts a stable (at the annual rate of 9%) growth of security market until 2016. As a result, the spending on security is expected to grow from $55 billion in 2011 to $86 billion in 2016 [5].

According to the *PwC Information Security Breaches Survey 2014* [6], for as many as 10% of the organisation whose security was violated the detriment of the violation was so severe that the organisations had to change the nature of business. The cost of individual security breach increased nearly two-fold in the UK in 2014 as compared with the previous year. In 2014, the average cost of the worst security incident for large organisations was in the range of £600,000 to £1,150,000. Small companies endured expenses between £65,000 to £115,000 for the worst security breach in 2014.

Over the last several decades, Information Security (InfoSec) has become a much diversified field of research and practice. Its scope has grown to include its filial discipline Information Assurance (IA).

In this thesis, the following definitions of InfoSec and IA are adopted:

Definition 1. ***Information Security*** *is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security countermeasures of all available types (technical, organisational, human-oriented and legal). The purpose of Information Security is to keep information in all its locations (within and outside the organisation's perimeter) and, consequently, an Information System (IS), where information is created, processed, stored, transmitted and destructed, free from threats.*

Definition 2. ***Information Assurance*** *is a multidisciplinary area of study and professional activity which aims to protect business by reducing risks associated with information and an IS by means of the comprehensive and systematic management of security countermeasures, which is driven by risk analysis and cost-effectiveness.*

These definitions were developed as a part of this research project, as the result of the literature analysis, and are presented in [7]. The discussion of the meaning and scope of InfoSec and IA is

continued in Chapter 2.

This thesis refers to the ***Information Assurance & Security*** (IAS) domain [8], which incorporates the knowledge of both InfoSec and IA.

For a long time, IAS has been considered as a purely technical issue and only computer and network specialists were involved in the discussion of security issues. At present, IAS is recognised as a complex managerial and organisation issue which requires knowledge of such disciplines as sociology, physiology, economics, management, marketing etc [49, 41]. The realm of IAS is not limited to the protection of electronic information, or to the technical side of it only. The scope of IAS includes all actions directed at keeping information secure as well as the management of these actions. IAS promotes an holistic approach to security where a sensible combination of security countermeasures of different nature is exploited for adequate information protection [49, 41].

1.1.2 Business Process. History and Significance.

"Business processes are at the core of organizations and an important success factor."
M. Weske [9]

A business process outlines a sequence of activities which should be undertaken by an organisation in order to achieve a business goal or desirable output. The role of business processes as a source of improvement and innovation is recognised by many organisations independently of size and domain [9].

The ideas related to business processes have been known in management for several centuries [10, 11]. A philosopher and economist Adam Smith (1723-1790) determined that a qualitative increase in productivity may be achieved through division of labour, when cooperating individuals specialise in the performance of certain tasks. A father of scientific management Frederick Taylor (1856-1915) promoted standardisation of methods, adoption of the best practices and cooperation. An American industrialist Henry Ford (1863-1947) invented mass production, where a large number of items are manufactured using an assembly line, where each person deals only with one operation, rather than the whole manufacturing cycle.

Business processes find their application in the contemporary management research and practice initiatives such as the Porter's value chain theory, Lean Management, Total Quality Management, Supply Chain Management, Activity-based Costing, Business Process Re-engineering and Six

Sigma [10, 12]. In the quality standards (e.g. ISO 9000-series, the European Foundation for Quality Management) business processes play a fundamental role: the standards require an organisation to document, follow and update its business processes on a regular basis [10].

In management, the roles of business processes are (1) the improvement of the understanding of business activities and their sequence, (2) the coordination of activities between participants of a process, (3) consensus building among various stakeholders involved in a process and (4) the enhancement of business performance. The statistics shows that the improvement of business processes has been one of the top priorities for management since 2005 [10]. The improvement of business performance does not necessarily involve ICT, but, in the majority of cases, ICT is a driver behind a business process change and innovation.

The advances of ICT in the last century revealed a new facet of business processes. Business processes outline instructions for automation in an IS. Thus, business processes, the importance of which from the management perspective is well known as discussed above, became critical from the perspective of IS designers and developers. Business processes play a strategic role at the early stage of the Information Systems Development Life Cycle (ISDLC) [13], in such approach as the Model-Driven Engineering (MDE) [14], for example. The role of business processes in the ISDLC is to outline functional requirements and to align the technical framework of an organisation with business needs. Software systems, where operational processes are managed and executed based on business process models are known as Process-Aware Information Systems (PAIS) [15]. Business processes are also exploited in the design of Service-Oriented Architectures (SOA) and web-services [16].

There are various definitions of a business process some of them focus on the transformation of an input into an output, others on the coordination of activities. The third group of definitions concentrates on the deployment of business processes [17]. The definition of a business process proposed by Weske in [17] (the key reference of the BPM domain) is adopted in this work:

Definition 3. *A business process consists of a set of activities that are performed in coordination in an organisational and technical environment. These activities jointly realise a business goal. Each business process is enacted by a single organisation, but it may interact with business processes performed by other organisations.*

The definition of a business process proposed by Weske is holistic and does not restrict the notion of a business process to any specific aspect. Furthermore, it explicitly refers to the interactions

between business processes of different organisations which is important to stress in the context of this thesis.

1.1.3 Cross-organisational Business Processes and Information Sharing

Cross-organisational business processes involve several organisations that work together in order either to achieve a common goal or to facilitate each other's businesses. Cross-organisational business processes have become widespread since they help organisations to be more effective and stay competitive on the global market [18]. Supply chains, including the global ICT supply chain, the collaboration between an organisation and service providers (outsourcing), the collaboration between an organisation and its business partners are a few examples of cross-organisational business processes. The statistics confirms a steady growth of outsourcing in the UK [6].

Cross-organisational business processes typically involve sharing sensitive information. A thorough consideration of IAS in cross-organisational business processes is critical [18, 19]. The sharing of sensitive information between different organisations poses multiple challenges: (1) information leaves the safe perimeter of an organisation, but still requires adequate protection while it is being stored, processed, transmitted or destroyed outside the organisation, (2) a security breach at one organisation may compromise other organisations involved in information sharing, (3) same information has dissimilar value for different organisations, and (4) information classification and labelling schemes of separate organisations often vary.

As an example of how widespread inter-organisational sharing is a typical Small and Medium-size Enterprise (SME), which sells stationary goods online may be considered. The web-site and the database of the SME are hosted externally by service provider who has access to the sensitive data. The SME closely cooperates with suppliers and shares information about goods, customers, orders and payments. The personnel of SME has access to the externally stored suppliers' databases of goods. In its turn, the SME provides suppliers with access to its own database which holds information about orders. As a result, the hard perimeter of the SME erodes. Larger companies have far more complex information sharing needs. The collaboration of the Boeing company with airplane owners and operators in order to address in-service issues is one of the examples of complex collaborative environment. Airlines, in general, which allows reservations on other companies flights through their own reservation systems and which share information about flights

and customers is another example. Another example is a joint product development project, when two or more companies have complex information sharing needs. Banking system is a possibly the best example: having money in one bank a customer could withdraw his/her money from a cash machine of another bank. All the above examples assume collaborative information sharing and the consequent erosion of hard organisations' perimeters.

This thesis, while taking into account intra-organisational business processes as well, focuses more on inter-organisational business processes where sensitive information is shared between different organisations. Inter-organisational information sharing is addressed in the conceptual model of the IAS domain and in a security modelling extension developed in this thesis.

1.1.4 Benefits of the Integration of IAS into Business Process Models

In 2014, the review of BPM publications identified addressing security issues as one of the three major challenges of business process modelling [20]. There are a large number of publications tackling the problem of security in business processes from various perspectives (Section 5.4.2). The importance of the consideration of security in business process is further confirmed by the existence of workshops on security in business process at the major conferences on BPM (e.g. Secure Business Processes workshop at the International Conference on BPM).

The incorporation of IAS modelling capabilities into a business process modelling language allows the realisation of several critical goals:

- the involvement of non-technical experts in the discussion of IAS issues,
- the engagement of senior management in the IAS decision-making,
- IAS is addressed at the early stage of the ISDLC, and
- IAS issues in inter-organisational processes are made more evident and the approach to IAS between organisations is harmonised.

Each of these goals is discussed in detail below.

Business process models provide a shared base for communication between business, IS and ICT experts [21]. The need for business and technical experts to be involved in the design of Secure Business Processes is well discussed in the existing research [22, 23]. However, the broadening

of the scope of IAS leads to a growth of the number of experts, who must be involved in the discussion of IAS and, consequently, in the design of secure business processes. The knowledge of experts with different, often non-technical, backgrounds which relates to the various aspects of IAS such as legislation, human-factor, administration, etc. must be captured in order to produce an holistic picture of IAS in an organisation. Business process models provide a basis for the representation of technical and non-technical IAS concerns in a graphical form and at the high level of abstraction easily accessible by a broad range of experts [24]. Hence, the consideration of security in business process models aids in engaging non-technical and non-security experts in security discussion and decision-making.

The representation of IAS concerns in business process models encourages the senior management engagement in security discussion and decision-making. This engagement is important because, in addition to capturing their security-related knowledge, it improves their understanding of security challenges and potential solutions. As a result, more competent security decisions are taken. Senior management also make the decisions about IAS programs funding. It is easier to convey and justify the importance of IAS to the management team who are well-informed about IAS.

Thus, business processes form a basis for the communication regarding IAS in which a wide range of experts irrespectively of their background may participate.

Addressing IAS in a business process model promotes the critically important integration of IAS into an IS at the earliest stage of the ISDLC. Business process models not only describe the order of activities, but capture a conceptual view of the business and its objectives. That is why business processes are well-positioned for the integration of security into the very “core" of an IS [22]. A necessity for security to be an integral part of an IS is declared in ISO/IEC 27001:2005 (A.12.1). ISO/IEC 27002:2005 (Sec. 4.2) states: “*Information security controls should be considered at the systems and projects requirements specification and design stage. Failure to do so can result in additional costs and less effective solutions, and maybe, in the worst case, inability to achieve adequate security*."

The consideration of security at the requirements formulation and design stages has not yet become a common practice. IAS is often treated as an afterthought and left until implementation [24, 25] which leads to security vulnerability and additional expenses. Business process models are developed at the early stage of the ISDLC in order to outline functional requirements. IAS modelling in business process models helps to overcome the “bolt on" attitude to IAS by enabling the specification of non-functional security requirements along with functional requirements [24].

The representation of IAS details in inter-organisational business processes improves the understanding of security issues, which emerge when sensitive information is shared among different organisations, because the flow of sensitive information is clearly depicted. While observing a security-annotated inter-organisational business process model from the perspectives of different organisations-participants, an observer will clearly see how information classification and labelling schemes, and often overall approach to IAS of the organisation-participants differ. Thus, the incorporation of IAS into business process models is a stepping stone on the way to the harmonisation of the approaches to IAS among organisations involved in information sharing. The harmonised approach to IAS is important because any organisation-information owner must ensure that its information is protected according to its security policies even when it is processed, transmitted or stored by other organisations.

1.1.5 Perspective and Approach

In this thesis, an holistic and systematic approach to IAS is adopted and promoted. An holistic approach to IAS in this research means that IAS is not limited to its technical aspect. IAS is considered as a complex managerial issue which may be addressed only by a sensible combination of security countermeasures of different nature (organisational, technical, human-oriented and legal).

A systematic approach means that IAS must be consistently addressed at all stages of the IS-DLC. The consideration of IAS at the stage of business process modelling is a part of an holistic systematic approach to IAS which provides a better guarantee for the completeness of security requirements and their better compliance with business goals. This thesis concentrates in detail on the consideration of IAS at the early stage of the IS design - the business process modelling stage.

This research is carried out in the context of the IS design and development. More specifically, this thesis proposes a means for the design of a *Secure* IS. In this context, the definition of an IS is important.

It is not a trivial task to produce an agreed definition of the term IS which is often used to refer to different objects [27]. In [27], over twenty definitions of an IS are considered. The focus of the definitions vary from social and organisational aspects to technical and mathematical ones. An IS, as it understood in this research, is not limited either to the technical or social perspectives. The combination of all perspectives defines its complex socio-technical nature. The following definition of an IS is adopted in this thesis:

Definition 4. *An **Information System** (IS) is a socio-technical system, which delivers information and communication services required by an organisation in order to achieve business objectives. An IS encompasses six components: (1) information (data), (2) people, (3) business processes (procedures), and ICT, which includes (4) hardware (5) software and (6) networks. An IS may interact with and be influenced by other ISs.*

This definition is based on the analysis of definitions of an IS presented in [27]. Six components of an IS are also listed in [28, p.17-19]. This definition highlights the complex nature of an IS. It does not limit an IS to the ICT components only.

No system exists in a vacuum: every system provides information and/or services to and receives them from external parties. Hence, the influence of the external world should be accounted for by an IS as pointed out in the definition.

1.2 Motivating Scenario and Problem Statement

The scenario that motivates this work and which is used throughout this thesis is as follows. A multidisciplinary group of experts discuss IAS issues in a specific business process. The team includes experts with technical and non-technical, security and non-security backgrounds:

- Business expert (manager or business owner),
- IAS officer,
- Computer and network expert (system administrator),
- Legal adviser and
- Human Resources (HR-)expert.

The specialisation of the experts is described in Appendix A.1. Depending on the size of an organisation and the nature of business other experts may also be involved. The need for the involvement of a large number of experts with different backgrounds is rooted in the multi-disciplinary nature of the IAS domain as discussed in Chapter 2.

The team observes a model of a business process. The model is developed prior to the discussion usually by or with the involvement of a business expert. It is out of the scope of this thesis to

consider how the process may be improved in aspects other than security. The team discusses the IAS-related details and issues in the business process and suggest countermeasures required to overcome the issues. After the discussion and model security-annotating are completed, the approved security countermeasures and recommendations are recorded in an Information Security Policy Document in the form of security statements.

This thesis tackles two problems which arise in this scenario.

First, although the experts involved in the discussion have security-related knowledge, which is manifested by the existing research [24], there is no effective notation allowing them to express their diverse knowledge within business process models in an unambiguous way.

The lack of such notation prevents the effective communication between experts involved in the design of Secure Business Processes[1]. The analysis of the existing extensions (Section 2.8) confirms a need for a security modelling technique which embraces the complex and heterogeneous nature of the IAS domain.

Since for the experts involved in the IAS discussion security is not their primary responsibility, they have only limited time to familiarise themselves with a notation. Therefore, a notation must be easy-to-learn and easy-to-use. It is anticipated that it shall be possible to learn a notation during 30-60 minutes training session. Ideally, an IAS modelling notation must be developed as an extension to an existing well-known business process modelling language because this will help to reduce learning time due to the fact that a large number of business and IS (and in some cases other domain experts as well) are usually familiar with business process modelling languages. Business Process Model and Notation (BPMN) 2.0 is the de-facto industry standard business process modelling language and the first international standard in business process modelling. BPMN 2.0 allows modelling of cross-organisational collaborative business processes. Therefore, BPMN is the logical choice as the basis for the IAS modelling extension. The advantages of BPMN are further discussed in Chapter 5. A need for extending BPMN for security modelling is argued in our earlier work [26], where it is demonstrated that (1) the syntax of BPMN 2.0 is not sufficient for IAS modelling and (2) none of the existing security BPMN extensions represents IAS concepts consistently.

[1] Secure business process in this work refers to a business process annotated with security information [29].

Since a notation is destined for humans comprehension (and not for the automatic interpretations as it often is in the related work) its cognitive effectiveness[2] becomes highly critical. Graphical annotations are better comprehended by humans [30, 31]. Therefore, an extension shall give preference to graphical annotations avoiding primarily machine-oriented text-based annotations.

Second, a multidisciplinary group requires an agreed-upon understanding of the IAS domain for an effective communication and meaningful annotations of business process models to take place. The experts, whose involvement in security discussions and decision-making is beneficial, often have different perception of the IAS domain and its main concepts. This is confirmed by our experience and by the survey of IAS practitioners which was conducted as a part of this research project [32]. Therefore, prior to starting a discussion on IAS issues and the annotation of business process models, a multi-disciplinary team has to build an agreed-upon understanding of the IAS domain. Assuring a commonly agreed understanding of IAS in cross-organisational teams of experts, who represent the interests of different members of an information sharing community, is also critical as it is a stepping stone on the way to harmonising the approach to IAS between the organisations involved in information sharing. This agreed-upon understanding of the IAS domain and the terminology must be employed as a basis for the semantics of a modelling notation. An agreed understanding of the IAS domain may be expressed in the form of a conceptual model. The completeness and accuracy of the conceptual model which is used as the basis for the semantics of a notation ensures the ontological completeness of the notation.

In the search for a conceptual model of IAS, which is to be exploited as the foundation for the semantics of a security modelling notation, the existing conceptual models of IAS were examined (Section 2.8) and the bases for the semantics of the existing security extensions for business process modelling languages were analysed (Section 5.4). Every examined model has some drawbacks and is not fully suitable for the purposes of this research project as in detail discussed in the above referenced sections of this thesis.

Finally, the problem addressed by this thesis may be summarised as follows:

There is a need for an easy-to-learn and easy-to-use graphical IAS modelling notation, which will be accessible by technical and non-technical, security and non-security experts alike. The semantics of a notation must be built upon a shared understanding of the IAS domain amongst the experts involved in the security discussion and decision-making.

[2] Cognitive effectiveness refers to the speed, ease and accuracy of the processing of a notation by people [30].

1.3 Research Objectives

The objectives of this thesis are:

Objective 1 : Develop a solution for the problem identified above. More precisely, to develop a modelling technique[3] that allows the representation of IAS concerns in business process models (Objective 1.A). The semantics of a modelling technique must draw upon a comprehensive conceptual model of the IAS domain which represents the domain in its contemporary state. A conceptual model shall represent IAS knowledge in the form suitable for a specific target audience - a multi-disciplinary group of experts. Since the existing literature does not provide a sought-for model of IAS, the model is to be developed in this research project (Objective 1.B).

Objective 2 : Evaluate the proposed IAS modelling technique (Objective 2.A) and the conceptual model of IAS, which underpins the semantics of the modelling technique (Objective 2.B). The evaluation must be conducted using well-established in the existing literature evaluation frameworks[4].

1.4 Proposed Solution and Hypotheses

This thesis proposes Secure*BPMN - a novel graphical security modelling extension for BPMN 2.0 which is designed for security annotation of business process models by a multidisciplinary team of experts.

The conceptual scheme of the proposed solution is depicted in Figure 1.1. The components which are innovative and developed in this research project, are shaded. The unshaded components illustrate the existing concepts.

[3] In this work the terms *modelling technique*, *modelling notation or language* are used interchangeably as synonyms.

[4] In this thesis the following evaluation frameworks are exploited: the quality criteria for conceptual models [33], the theory for visual notation design [30], the representation model [34, 35, 36] and the method evaluation model [37]. The descriptions of these frameworks, along with the justification of the choice, are outlined in Chapters 4 and 7 in which the evaluation of the developed reference model of IAS and of the proposed modelling technique are respectively contained.

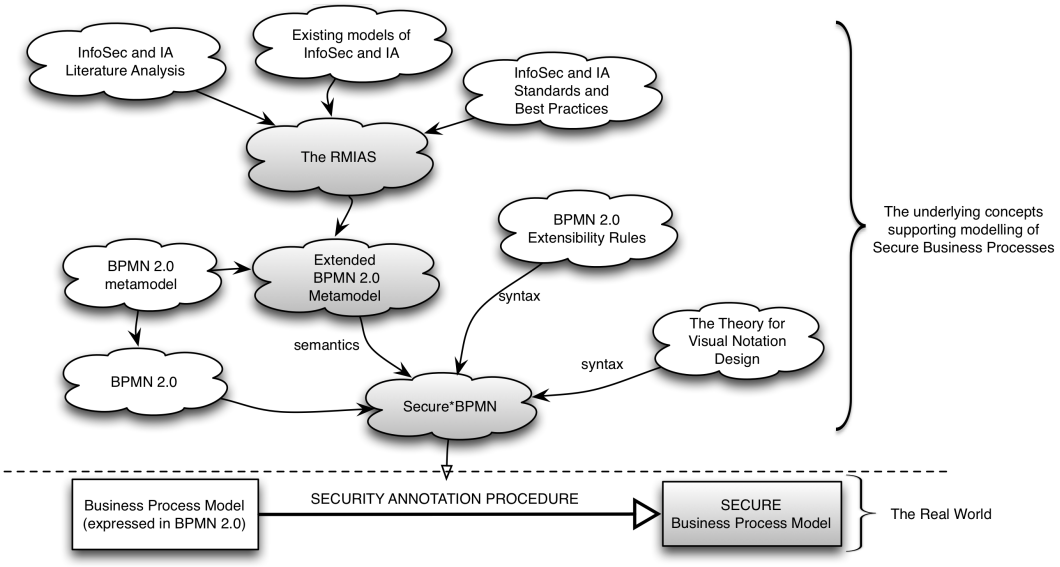


Figure 1.1: The general concept behind Secure*BPMN

Figure 1.1 shows that a business process model shall go through a security annotation procedure in order to become a Secure Business Process Model. Secure*BPMN is a modelling technique which provides a tool for security annotation of business process models expressed in BPMN 2.0. The semantics[5] of Secure*BPMN draws upon a Reference Model of Information Assurance & Security (RMIAS) which was developed in the frame of this project. The syntax of Secure*BPMN is guided by the BPMN extensibility rules and the Theory for Visual Notations Design (TVND) [30] which declares the principle for the design of cognitively effective notations.

Secure*BPMN and the RMIAS are claimed to solve the problems outlined in Section 1.2.

Evaluation is critical for any research claiming plausibility. This research was strongly focused on the evaluation of the proposed solution. Considerable effort and time were devoted to the analytical and empirical evaluation of the different aspects of the proposed solution. The details of the exploited evaluation methods are outlined in Section 4.1 and Chapter 7 for the RMIAS and Secure*BPMN respectively.

There are two hypotheses which are tested in this thesis.

Hypothesis A: *Secure*BPMN is an ontologically complete and cognitively effective modelling notation which is perceived by experts with different backgrounds and with the different levels of*

[5]The structure of a visual notation is described in Appendix A.2.

experience in IAS and BPM as a useful and easy-to-use IAS modelling technique which is likely to be adopted in practice.

Hypothesis A tests how well Secure*BPMN meets the criteria of an effective modelling notation and evaluates the likelihood of its adoption in practice.

Hypothesis B: *The RMIAS provides more complete and accurate representation of the IAS domain, than the existing conceptual models of the IAS domain. The RMIAS reflects how the IAS domain is understood by IAS domain experts. It represents the domain in the form accessible by the experts with the different backgrounds and with the different levels of experience in IAS. Due to the above, the RMIAS helps to build a congruous understanding of the IAS domain in a multidisciplinary team of experts and provides a solid basis for the semantics of Secure*BPMN.*

Since the RMIAS underpins Secure*BPMN it is critical to check the quality of the RMIAS. Hypothesis B aims to test whether the RMIAS corresponds with the vision of IAS possessed by the experts of this domain and whether the RMIAS meets the quality criteria of a conceptual model, namely simplicity, accuracy, scope, systematic and explanatory power, reliability, validity and fruitfulness..

Figure 1.2 depicts the evaluation process - the evaluated parameters, methods used for the evaluation and the theoretical frameworks underlying the evaluation.

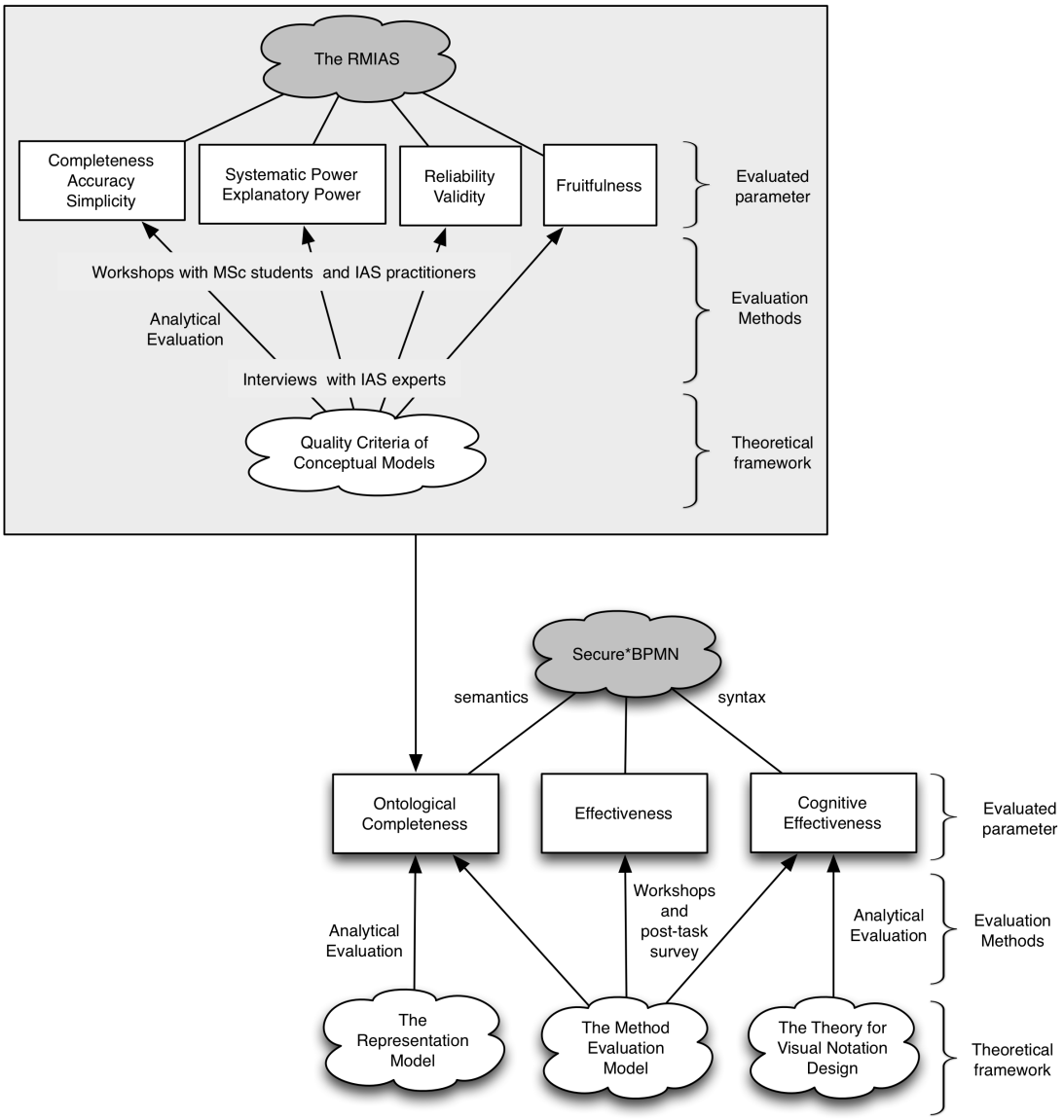


Figure 1.2: The evaluation of Secure*BPMN and the RMIAS

1.5 Research and Development Method

Secure*BPMN and the RMIAS were developed and evaluated in six steps which are outlined below.

Step 1 - Understanding the IAS domain

The InfoSec and IA literature (standards, industry and academic publications) were examined and the analysis is presented in [7]. A survey of InfoSec and IA practitioners aimed at the identification

of security goals associated with InfoSec and IA was conducted [32]. Based on the analysis, the adapted definitions of InfoSec, IA and IAS were developed [7]. A systematic analysis of the existing models/frameworks of InfoSec and IA was carried out. This analysis confirmed a need for the development of an updated conceptual model of IAS.

Step 2 - The Development of the RMIAS

The knowledge representation was researched and a reference model as the form of representation of the IAS domain knowledge was chosen. Based on the literature analysis four dimensions of the RMIAS were identified and each dimension was elaborated in detail. Then, the interrelationships between the dimensions and drivers behind the IAS decisions were identified. The RMIAS, which is presented in Chapter 3, is the outcome of this step.

Step 3 - The Evaluation of the RMIAS

A multiphase evaluation methodology was developed and evaluation quality criteria for the RMIAS were chosen. The interviews with InfoSec, IA and business experts were conducted to test how well the RMIAS meets the quality criteria. The workshops with practitioners and MSc students took place to test the practical value of the RMIAS. A case-study corroborated the validity of the RMIAS. The RMIAS evaluation results corroborated the adequacy and completeness of the RMIAS and, therefore, confirmed that the RMIAS is suitable to be exploited as a basis for the semantics of Secure*BPMN.

Step 4 - Understanding the BPM domain and the integration of IAS into it

The BPM domain and its main concepts were researched. The analysis of the existing security extensions for business process modelling languages was conducted. BPMN 2.0.1 was chosen to serve as a basis for the extension. The BPMN extensibility rules were examined. The RMIAS was aligned with BPMN to show that BPMN requires an extension [26]. The existing security and risk extensions for BPMN were examined in detail.

Step 5 - The Development of Secure*BPMN (semantics, syntax and annotation procedure)

The BPMN metamodel was extended with the constructs extracted from the RMIAS. A framework to guide the design of Secure*BPMN was selected and the syntax was designed. The Secure*BPMN annotation procedure and an annotated example were elaborated. The Secure*BPMN stencils for Mac OS OmniGraffle and Microsoft Visio 2010 were developed. The outcome of this step was Secure*BPMN.

Step 6 - The Evaluation of Secure*BPMN

The frameworks for the analytical evaluation of Secure*BPMN were chosen. The analytical evaluation of Secure*BPMN was conducted. The procedure and supporting materials for the empirical evaluation of Secure*BPMN were elaborated. The workshops with practitioners and MSc students were conducted to test the effectiveness of Secure*BPMN. The results of the empirical evaluation were analysed. At this step, the cognitive effectiveness, ontological completeness of Secure*BPMN were confirmed as well as its ease of use and usefulness. The likelihood of its adoption in practice was analysed.

1.6 Structure of the Thesis

The structure of the thesis reflects the development method and is presented in Figure 1.3.

Each chapter starts with a short introduction which explains what a reader will find in the chapter and how the chapter links to the previously presented material. Each chapter ends with a summary which recapitulates the material presented in the chapter and shows how the chapter contributes to the research objectives and hypotheses.

Chapter 1 introduces the reader to the research conducted in the frame of this PhD project. It explains the problem being addressed, outlines the research context and research hypotheses. The research and development methodology is presented in this chapter. The main contribution of this research is explained.

Chapter 2 investigates the IAS domain, identifies its scope and goals, and develops the approach to IAS upon which the RMIAS is then developed. This chapter also presents the analysis of the existing models/frameworks of IAS.

Chapter 3 presents the RMIAS. First, the chapter gives a brief introduction to knowledge formalisation and justifies the choice of a reference model as the form of IAS knowledge representation. Then, the chapter gives an overview of the RMIAS which is then followed by the detailed description of each dimension of the RMIAS. The wider implications of the RMIAS are also discussed in this chapter.

Chapter 4 outlines the multi-phase evaluation methodology which is used for the evaluation of the RMIAS. It outlines the set up of the evaluation experiments and discusses the evaluation results.

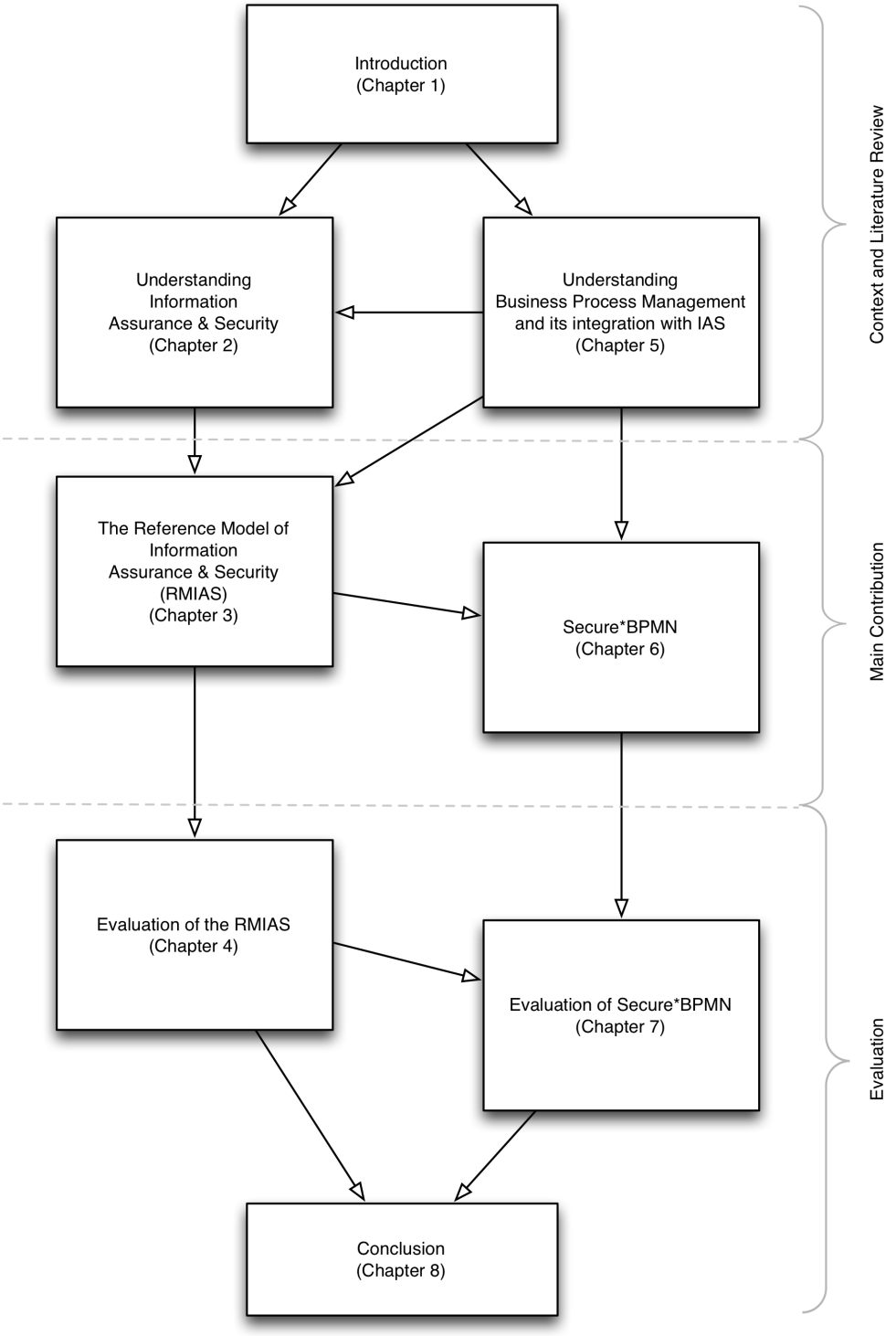


Figure 1.3: The structure of the thesis

Chapter 5 gives the reader more insight into BPM. The perspective on business processes adopted in this thesis is clarified thorough the chapter. This chapter also presents the analysis of the existing

security extensions for business process modelling languages and points out their drawbacks.

Chapter 6 introduces the semantics and syntax of Secure*BPMN. The BPMN metamodel is extended with the constructs extracted from the RMIAS. This chapter also outlines the annotation procedure, which should be followed when using Secure*BPMN, and gives an illustrative annotation example. The Secure*BPMN stencils for MS Visio and OmniGraffle are also presented in this chapter.

Chapter 7 is devoted to the evaluation of Secure*BPMN. The chapter contains the detailed analysis of the analytical and empirical evaluation results.

Chapter 8 summarises the results of this research project and discusses future work.

The research and development was conducted in an iterative, rather than a strictly sequential manner. The arrows in Figure 1.3 illustrate the logical dependencies between the chapters of the thesis. For example, the development of the RMIAS was prompted not only by the analysis of the IAS domain (Chapter 2), but also by the analysis of the existing extensions to business process modelling languages in (Chapter 5).

1.7 Contribution of the Thesis

This thesis is a contribution to both IS and IAS research.

The major contribution of this thesis is Secure*BPMN - a graphical IAS modelling extension for BPMN 2.0. Secure*BPMN helps to create an holistic view of security issues in a business process. Secure*BPMN enables the design of secure business processes in a graphical way, which is more accessible by a non-technical audience. Secure*BPMN enables effective representation of security concerns in business process models and, by doing so, it facilitates the engagement of non-security and non-technical experts in the discussion of security concerns and security decision-making. Consequently, the use of Secure*BPMN leads to the better informed and more optimal security decision and, as a result, to the greater degree of information security. Secure*BPMN allows the representation of security concepts in both intra- and inter-organisational business process models.

The strength and novelty of Secure*BPMN lies in its cognitively effective syntax and, primarily, in its comprehensive semantics based on the RMIAS.

The RMIAS is a synthesis of the existing knowledge of the IAS domain. It was developed as a result of a thorough literature review. The RMIAS helps to build an agreed-upon understating of the IAS domain (its main concepts and the interrelationships between them), which a multidisciplinary team requires before experts may proceed with the discussion of security issues.

The novelty of the RMIAS is in synthesising the discrete knowledge at a high level of abstraction in one all-encompassing model. The RMIAS provides a way of structuring the IAS knowledge accessible to technical and non-technical audience. The RMIAS conveys the diverse nature of IAS and its understanding as a complex organisational issue.

The RMIAS is declared as a secondary contribution of this thesis as the primal purpose of the thesis is to develop an IAS modelling notation. The RMIAS in this thesis is exploited as a basis which underpins the semantics of Secure*BPMN. However, the evaluation of the RMIAS confirms that the RMIAS has multiple applications apart from forming a basis for the semantics of an IAS modelling technique. The RMIAS, which has multiple implications for research, education and practice (Sections 3.12.2) is a contribution to the IAS domain in its own right.

Overall, this thesis provides a means that helps to design IAS into an IS from an early stage of the system development life cycle. This prevents security being treated as an afterthought in an ad-hoc manner. The thesis also introduces a reference model for structuring and harmonising the approach to IAS among all experts involved in the design of secure IS.

In addition to the proposed solution, this thesis develops and exploits a multiphase evaluation procedure for both a modelling notation and a reference model. The evaluation procedures employed may be of interest for researchers, particularly because they may serve as bases for comparative studies.

In this thesis, the related literature which cluster around two research areas is examined in depth. First, conceptual models and frameworks of IAS are analysed. Second, security extensions for business process modelling languages are examined. While some analysis of security extensions may be found in other publications, to the best of the author's knowledge there is no other publications which analyse conceptual models of IAS in such depth.

1.8 Publications and Talks

This PhD research resulted in a number of publications and conference contributions which are listed below:

Book Chapters

[*1] Y. Cherdantseva and J. Hilton, "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals," In: F. Almeida, and I. Portela (eds.), Organizational, Legal, and Technological Dimensions of IS Administrator. IGI Global Publishing. September, 2013.*

This book chapter contains an extensive analysis of InfoSec and IA literature which culminates in the adapted definitions of both domains. This book chapter also discusses security goals associated with InfoSec and IA and concludes that an extended list of security goals must be developed in order to address the broad scope of the IAS domain. The approach to IAS which is adopted in this thesis draws upon this analysis. This book chapter also argues a need for a new reference model of the IAS domain.

[2] Y. Cherdantseva and J. Hilton, "The 2011 Survey of Information Security and Information Assurance Professionals: Findings," In: F. Almeida, and I. Portela (eds.), Organizational, Legal, and Technological Dimensions of IS Administrator. IGI Global Publishing. September, 2013.

This book chapter debates the results of the survey of IAS practitioners. The purpose of the survey was to establish how practitioners understand InfoSec and IA. The results of the survey manifest that practitioners are often uncertain about the scope and goals of InfoSec and IA due to the continuous changes of them. Thus, the results of the survey, among other conclusions, also prove a need for an updated model of the IAS domain.

Conference Papers

[3] Y. Cherdantseva, O. Rana, J. Hilton, "Security Architecture in a Collaborative De-Perimeterised Environment: Factors of Success," ISSE Securing Electronic Business Processes, Prague 22-23 November 2011. Highlights of the ISSE 2011 Conference, pp. 201-213. 2011.

This paper investigates the specifics of IAS in the environment where sensitive information is shared cross-organisationally. The analysis of the literature presented in this paper helped to set a research direction for this thesis. Thus, this thesis pays special attention to cross-organisational information sharing.

[*4] Y. Cherdantseva, J. Hilton, O. Rana, "Towards SecureBPMN - Aligning BPMN with the Information Assurance & Security Domain," In: Mendling, J. and Weidlich, M. (eds.) Business Process Model and Notation (BPMN) 2012. LNBIP, vol.125, pp.107-115. Springer, Heidelberg, 2012.*[6]

This paper is devoted to the argument about why BPMN needs a security extension. The paper also outlines the Secure*BPMN development method. During the presentation at BPMN 2012 conference, the first version of the Secure*BPMN syntax was presented and the useful feedback, which was addressed in the later versions of the notation, was received.

[5] Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance & Security," Availability, Reliability and Security (ARES), 2013 Eighth International Conference on , vol., no., pp.546-555, doi: 10.1109/ARES.2013.72, 2-6 September, 2013.

This paper introduces the RMIAS. At the ARES 2013 conference the RMIAS was well accepted by the security ontology community. The participants of the workshop - practitioners and researchers - appreciated the merit of the RMIAS and positively appraised the applicability of the RMIAS in practice.

Talks

During the project, the research presented in this thesis was actively communicated to various audiences. Over 10 talks related to different aspects of this research were given to PhD students, MSc students specialising in Information Security & Privacy and academics at the School of Computer Science & Informatics, Cardiff University; to MSc students specialising in Cyber Defence and Information Assurance at Cranfield University and to the Software Engineering Research Group (SERG) at University of the West of England.

[6]In 2012, Secure*BPMN was originally presented under the title SecureBPMN. In the same year, another publication [38] by a different group of authors emerged with the similar title. In order to avoid confusion while retaining the identity, the original title SecureBPMN was later changed to Secure*BPMN.

Chapter 2

Understanding Information Assurance & Security

The importance of IAS is manifested by statistics and by many references as discussed in Chapter 1. Despite the great interest in Information Security (InfoSec) and Information Assurance (IA), there is still no commonly agreed understanding of these disciplines. Every author makes a unique interpretation of InfoSec and IA by identifying the divergent scopes and goals of the disciplines. The approaches to InfoSec and IA vary, depending on the background of an author and on the nature of the author's occupation. In this research, it is important first to establish the scope of the IAS domain in order to empower the development of a conceptual model of the domain which will form a foundation for the semantics of a security extension for a business process modelling language. This chapter delves deeper into the IAS domain in order to establish the domain's scope and goals. This chapter investigates InfoSec and IA literature, and presents the definitions of the disciplines which are adopted in this thesis. It also overviews the recent trends in the evolution of IAS. A notion of a security goal is demonstrated to play a key role in the IAS domain. Then, after a discussion of the importance of a conceptual model of IAS and a need for its regular revision, this chapter presents a dissection of the existing conceptual models and frameworks of IAS.

2.1 Information Security

This section contains a detailed analysis of the term InfoSec. First, an analysis of the term based on common English is conducted. Second, the definitions of the term as suggested in the official standards are discussed. Third, the understanding of InfoSec in academic and industry publications is researched, and the latest trends in InfoSec are distilled. Finally, an adapted contemporary definition of InfoSec is presented and discussed.

2.1.1 Common English

Formal or academic definitions are often distinct from the common comprehension of terms [122, 66]. In order to understand the common perception of the term InfoSec we start from the definitions of isolated words *information* and *security* in the [39] (the definitions are abridged):

- Information n.
  1. knowledge acquired through experience or study;
  2. computing
     a. the meaning given to data by the way in which it is interpreted
     b. another word for data.
- Security n.
  1. the state of being secure;
  2. precautions taken to ensure against theft, espionage, etc.

Secure is defined as *"free from danger, damage, etc; not likely to fail; able to be relied on"* [39]. Precaution is defined as *"an action taken in advance to prevent an undesirable event"* [39]. The [40], in turn, defines security as *"the state of being free from danger or threat"*. Based on the above, a general definition of InfoSec could be derived:

Information Security is a discipline, the main aim of which is to keep the knowledge, data and its meaning free from undesirable events, such as theft, espionage, damage, threat and other danger. Information Security includes all actions, taken in advance, to prevent undesirable events happening to the knowledge, data and its meaning so that the knowledge, data and its meaning could be relied on.

In the general definition of InfoSec five points should be highlighted. First, there are no restrictions on the information type. In the broad sense, InfoSec is concerned with information of any form or type (e.g. electronic, paper, verbal, visual). Second, InfoSec includes *all* actions to protect information. Thus, InfoSec is concerned not only with technical actions, but deals with the full diversity of protecting actions required during information processing, storage or transmission. Third, the list of undesirable events is broad and open. The definition explicitly lists theft, espionage and damage of the information, but is not restricted to them. Thus, InfoSec deals with the protection

of information from *all* undesirable events. Fourth, the general definition of InfoSec does not state any security goals such as confidentiality, integrity, availability or any other. Therefore, in line with the third point, the main aim of the discipline is the overall protection of information, and not just the achievement of several pre-defined security goals. Fifth, InfoSec includes actions taken *in advance*. Therefore, InfoSec should be concerned not only with an analysis of undesirable events, which have already taken place, but also with the anticipation of such events and an assessment of the their likelihood.

2.1.2 Official Documents

There is a plethora of standards covering the various aspects of InfoSec published by international organisations (ISO, IEC, ITU), national standards bodies (BSI, NIST, SAA, SNZ, JISC), non-profit organisations (ISACA, ANSI, IEEE, OMG, OASIS, ETSI) and international communities (IETF, W3C, EEMA, Wi-Fi Alliance, ISF).

In this section the definitions of InfoSec provided in the vocabulary of the ISO/IEC 27000 series [55] and in the National Information Assurance Glossary [56] are analysed, and compared to the definition suggested by ISACA [57].

The ISO/IEC 27000 series of standards is an internationally recognised and widely adopted InfoSec standard. The series was developed by a joint committee of the International Organisation for Standardisation (ISO) and the International Electronic Commissions (IEC) and covers InfoSec management, InfoSec risk management, implementation of InfoSec Management Systems (ISMS), measurements and metrics of ISMS. In 2000, the ISO adopted BS7799, the standards published by the British Standard Institute in 1995, under the name ISO/IEC 17799. BS7799 was based on the Code of Practice for Information Security Management, which was developed by the Department of Trade and Industry in close rapport with leading UK organisations. In 2007, ISO/IEC 17799 was incorporated in the ISO/IEC 27000 series as ISO/IEC 27002.

The National Information Assurance Glossary, published by the Committee on National Security Systems (CNSS), is also known as the CNSS Instruction 4009 (CNSSI) [56]. The glossary was created to resolve the differences between the definitions of terms used by the U.S. Department of Defense (DoD), Intelligence Community and National Institute of Standards and Technology Glossary (NIST). NIST develops U.S. Federal Information Processing Standards publications (FIPS PUB). The standards are primarily oriented on the government systems, but are also useful

for industry.

ISACA is a non-profit, global association of over 95,000 members worldwide. It develops practices for information systems. ISACA is an originator of the globally accepted Control Objectives for Information and related Technology (COBIT) framework.

The definitions of InfoSec suggested in the three documents mentioned above are summarised in Table 2.1, along with the definitions of integrity, which are discussed later in this section.

Table 2.1: Definitions of Information Security and Integrity

Term Standard	Information Security	Integrity
[55]	Preservation of confidentiality, integrity and availability of information. Note In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.	The property of protecting the accuracy and completeness of assets.
[56]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.	The property whereby an entity has not been modified in an unauthorized manner.
[57]	Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability).	The accuracy, completeness and validity of information.

The official definitions of InfoSec presented in Table 2.1 differ from the general definition (Section 2.1.1) and are inconsistent with each other. For example, the CNSSI definition includes in the scope of InfoSec protection of information systems, as well as information. An information system according to the CNSSI is defined as *"a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information"*. Thus, *information resources* are in the scope of InfoSec according to the CNSSI definition, but this is explicitly captured neither in the general definition of InfoSec, nor in the definition suggested by the ISO/IEC.

Both, the CNSSI and ISO/IEC 27000 define InfoSec based on a set of security goals to be achieved.

Thus, the essential discrepancy between the general comprehension of InfoSec and the definitions provided in the standards is that the general definition implies that information is secure if it is protected from all threats, whereas the standards imply that the information is secure if it complies with the certain security goals. This refers back to the fourth point stated in Section 2.1.1.

According to the definitions in Table 2.1, the scope of InfoSec defined by the ISO/IEC is wider than the scope defined by the CNSS. Apart from confidentiality, integrity and availability, the ISO/IEC also includes reliability, accountability, authenticity and non-repudiation in the realm of InfoSec, while the CNSS does not. For example, the breach of non-repudiation does not relate to any of the undesirable events stated in the CNSS definition. It is not mentioned in the CNSS definition of InfoSec as a security goal either.

Although the set of security goals associated with InfoSec in the CNSSI and ISO/IEC 27000 standard vary, they agree that the three fundamental goals of InfoSec are confidentiality, integrity and availability. ISACA clearly reflects this concept in its definition of InfoSec (Table 2.1). Consequently, the COBIT framework restricts the sphere of InfoSec to issues related to confidentiality, integrity and availability.

Since the standards correlate InfoSec with a certain set of security goals, then the origins of the goals and their interpretation becomes extremely important. The straightforward logical consequence of the steps to define an absolute list of security goals should be as follows: 1) identify all possible threats to information; 2) categorise the threats; 3) define a security goal for each category of threats. Due to the constant change in the environment, new threats constantly emerge and information received at the first step quickly becomes obsolete. Thus, security goals are only valid for the environment at a certain stage. This highlights the inadequacy of defining InfoSec purely through security goals, because any set of goals rapidly becomes incomplete in a transforming landscape and some threats stay out of the realm of InfoSec.

The definitions provided in the standards are used to define organisation's InfoSec program, strategy and policies. The limitation of InfoSec in this context leads to undesirable consequences that stem from overlooking essential threats and critical vulnerabilities that stay below the radar of InfoSec [66].

Defining the scope of InfoSec through certain security goals gives rise to two problems. First problem is the differing interpretations of the goals. The ISO/IEC 27000 standard and CNSSI definitions of *availability* and *confidentiality* correspond with each other, but the approaches to *integrity* in these two standards differ. The comparison of the definitions of integrity in Table 1

shows that the CNSS is concerned with the authenticity of data, while the ISO/IEC concentrates on the state of data, characterised by completeness and accuracy. Second problem: the CNSSI definition of InfoSec includes in its scope both information and information systems and, therefore, considering integrity in the definition of InfoSec, it is not clear whether it is integrity of information, or integrity of an information system, or both. If it is integrity of an information system, then to which part of the system it refers to: hardware, software, personnel or procedures.

In comparison to the general definition of InfoSec, the definitions suggested in the documents discussed narrow down the scope of the discipline because they define confidentiality, integrity and availability as the fundamental goals of InfoSec, rather than an overall protection of information. In the foreword to the first edition of Anderson's *Security Engineering* Schneier, wrote: *"You have to consider all the ways your system can fail... You have to look at everything backwards, upside down, and sideways*" [49, Foreword]. It is obvious now that the ways a system can fail could not necessarily be characterised by a breach of confidentiality, integrity or availability. A definition of InfoSec, which is restricted to a certain set of security goals, prevents security specialists from having the necessary broad view of InfoSec. Therefore, the focus on the achievement of several pre-defined security goals, rather than on the achievement of adequate security is a flawed and dangerous approach, since it may lead to an oversight of some threats.

In Section 2.1.3, it is discussed how academics and practitioners overcome the narrowing down of InfoSec to the CIA-triad (confidentiality, integrity and availability). An overview of the comprehension of InfoSec in the academic and industry publications of the last twenty years is presented. The recent trends in the evolution of InfoSec are distilled in Section 2.4.

2.1.3 Academic and Industry Publications

Significant research was conducted over the last twenty years in order to establish the scope and to clarify the goals of InfoSec. Nevertheless, there is still no single commonly-agreed definition of InfoSec. The challenge of defining the scope and the goals of InfoSec stems, firstly, from the complexity of the discipline, secondly, from a variety of approaches to the discipline and, thirdly, from the evolving nature of the discipline.

Traditionally, InfoSec is defined via a set of security goals. Since the late 1970s, InfoSec has been rigorously associated with the CIA-triad [28]. The major problem that arises from defining InfoSec via security goals is that the definition becomes obsolete as soon as new threats, not addressed by

any of the existing security goals, evolve.

In recent years, there is a pronounced tendency to extend the scope of InfoSec beyond the CIA-triad since the latter is found to be no longer adequate [28, 66] for a complex interconnected environment. A plethora of security goals is considered to be relevant to InfoSec and intensively discussed in the literature. Table 2.2 lists security goals associated with the discipline in the security-related publications. The publications are listed on the vertical axis in the chronological order. The horizontal axis lists security goals.

Table 2.2: Analysis of the literature in terms of goals associated with Information Security.

Reference	Confidentiality	Integrity	Availability	Accountability	Assurance	Authentication	Non-repudiation	Authenticity	Reliability	Effectiveness	Efficiency	Compliance	Utility	Possession/Control	Authorisation	Awareness	Access	Identification	Accuracy	Administration	Information Classification	Anonymity	Audit	Safety	Other (not specified)
[76]	X	X	X																						
[206]	X	X	X																						
[65]	X	X	X																						
[66]	X	X	X					X					X	X											
[42]	X		X	X											X	X	X	X	X	X					
[207]		X				X															X	X	X		
[208]	X	X	X	X	X																				
[209]	X	X	X				X	X																	
[269]	X	X	X						X															X	
[137]	X	X	X	X			X	X	X																
[64]	X	X	X						X	X	X	X													
[211]	X	X	X	X		X									X						X				
[57]	X	X	X																						
[216]	X	X	X																						
[55]	X	X	X	X			X	X	X																
[217]	X	X	X																						X
[56]	X	X	X			X	X																		
[43]	X	X	X																						
[174]	X	X	X	X			X																		
[218]	X	X	X																						
[28]	X	X	X					X					X	X					X						

The analysis demonstrates the lack of an agreement about security goals and, consequently, about the scope of InfoSec. The variety of security goals discussed in the literature leaves the scope of InfoSec ambiguous. Moreover, the problem with varying definitions of the same security goals is also present in the academic publications, similar to the official documents, as discussed in Section 2.1.2.

The lack of clear InfoSec terminology gives rise to another problem: security goals are not clearly distinguished from security countermeasures. A clear distinction between a *security goal* and a *security countermeasure* is required, as well as the association of a security countermeasure with a certain security goal. This may enable the easier choice of an appropriate mechanism to pursue a certain security goal. This calls for a comprehensive model of InfoSec that helps to resolve these issues.

Going deeper into the discussion of security goals associated with InfoSec, it is important to highlight a substantial contribution to the clarification of InfoSec done by [66]. Parker criticises the InfoSec definitions of being limited to the CIA-triad and claims them being dangerously incorrect. Parker introduces a new model of InfoSec that consists of six foundation elements: *confidentiality*, *integrity*, *availability*, *possession or control*, *authenticity* and *utility*. (Later, Kabay suggested the term *Parkerian Hexad* for the model, as a sign of respect to Parker.)

Possession or control is defined by Parker as *"the holding, control, and ability to use information"*. Consideration of possession as an additional security goals gains particular importance at the time of Cloud Computing. Utility is defined as *"usefulness of information for purpose"*. The definition of authenticity suggested by Parker, is much wider than the definitions of the same term provided in [56] and [55]. A comparison of the definitions is presented in Table 2.3.

Table 2.3: Definitions of Authenticity

Standard/Term	Authenticity
[55]	Property that an entity is what it claims to be.
[56]	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
[66]	Validity, conformance, and genuineness of information.

The definitions in the ISO/IEC 27000 standards and CNSSI correlate authenticity with the ability to verify the identity of the author. According to Parker, authenticity reflects *"the conformance to reality"* and *"extrinsic value or meaning of the information with respect to external sources"*. Parker states that even information provided by an authorised user, whose identity has been verified, may not necessarily comply with authenticity. That, for example, may happen in the case when an authorised user misrepresents information.

Parker [66] argues that his model replaces the incomplete description of InfoSec limited to the CIA-triad. Albeit the model of InfoSec, suggested by Parker [66], is not widely accepted, the research undertaken is fruitful because it addresses three issues, essential for the clarification of InfoSec:

1. The focus of the discipline is set on protection of information, rather than on protection of an information system. Parker consistently includes in his model properties of information and does not mix them with security countermeasures;

2. The importance of a complete and accurate definition of the discipline and, consequently, of the discipline's goals is highlighted and justified;

3. An attempt to extend the model of InfoSec and to address the limitations of the CIA-triad is undertaken. The overstepping the CIA-triad leads to the switch of InfoSec from the technical to the multidimensional discipline.

In agreement with Parker, Anderson [49] confirms that InfoSec is more than the CIA-triad. Anderson proclaims a multidimensional approach to InfoSec and sets forth that people, institutional and economic factors are no less important than the technical ones. Describing a security specialist, Anderson propones the requirement for such a specialist today to be familiar with business, management, and accountancy in addition to technology in order to be able to communicate effectively with the top management as well as with the technical staff.

Anderson also is a pioneer of security economics. The economic perspective of security has been intensively discussed since the turn of the XXI century. Anderson [44] conducted an analysis of economic incentives behind some InfoSec failures and concluded that a purely technical approach to InfoSec is ineffective . Further, Anderson states that collaboration between managers, economists and lawyers is required in order to solve problems related to InfoSec. While Anderson [44] provides the general inside view on the economic incentives behind InfoSec, Gordon and Loeb [209] look at the economics of investments into InfoSec. In 2002, they proposed the economic model that helps to determine the optimal amount of investment in InfoSec. In their work, Gordon and Loeb associate InfoSec with such goals as confidentiality, availability, authenticity, non-repudiation and integrity of information [209, p.439]. The importance of economic motives is also recounted by Schneier [45], who states that the number of vulnerabilities may only be reduced *"when the entities that have the capability to reduce those vulnerabilities have the economic incentive to do so"*. In addition to economics, Schneier reveals consideration of physiology and

management to be essential for InfoSec [45, 207]. Thus, in line with Anderson, Schneier confirms the multidimensional nature of InfoSec.

Schneier [207] describes InfoSec as a process that includes: understanding of threats, design of polices and building of countermeasures to address the threats and, further, states that all the components of the process must fit together in order to achieve a best state of the overall process. He distinguishes the following goals of InfoSec: privacy, information classification (referred to as multilevel security), anonymity, authentication, integrity and audit [207]. Schneier lists among security goals not only properties of information (as it was consistently done by Parker [66]), but also security countermeasures or abilities of information systems (e.g. authentication).

In line with Schneier, Pipkin [42] defines InfoSec as a process, in this case as *"the process of protecting the intellectual property of an organisation"*. Pipkin includes in the scope of InfoSec and discusses in detail ten security goals: awareness, access, identification, authentication, authorisation, availability, accuracy, confidentiality, accountability and administration. This is another confirmation of a wide trend in InfoSec to combine security goals and security countermeasures as a result of considering information and information systems simultaneously to be subjects of protection in InfoSec.

Importantly, Pipkin [42] takes InfoSec outside the hard perimeter of an organisation by defining that information should be protected *"in all its locations"*. In the present complex collaborative environment, information often intentionally leaves the safe boundaries of an organisation, but still requires protection. Pipkin [42] also highlights a necessity of InfoSec flexibility in a constantly evolving environment.

Pipkin unveils InfoSec from the business standpoint and argues a need for InfoSec to become a business enabler and an integral part of a business. A similar approach to InfoSec is presented by Sherwood et al. [41] who states that at present InfoSec, unfortunately, is often understood as a business preventer rather than a business enabler. According to Sherwood et al. [41], InfoSec may help to raise trust of an organisation by customers and partners, and to allow an organisation to use effectively newly emerging technologies for a greater commercial success. InfoSec enables business by increasing its competitiveness. Delving deeper into the business approach to InfoSec, it should be understood that security of information is required not for its own sake, but for the advantages it gives to business (e.g. improved efficiency due to the exploitation of new technologies, increased trust from partners and customers). Sherwood et al. [41] adopt a multidimensional and enterprise-wide approach to InfoSec and include in the scope of InfoSec, for example, such aspects

of business as marketing and customer service. The authors declare protection of business assets and assistance with the achievement of business goals to be the main aim of InfoSec. Sherwood et al. [41], in greater detail than Pipkin [42], addresses the change of InfoSec approach related to the erosion of the hard perimeter of an organisation caused by active collaboration, operation in a distributed environment, and outsourcing of IT and other services. Pipkin [42] and Sherwood et al. [41], by the adoption of a business-oriented approach, support the tendency to extend the realm of the discipline. Thus, InfoSec is no longer considered purely from a technical perspective, but also from a managerial, system architect's and designer's points of view.

In line with others, Von Solms [47] confirms the transition of InfoSec from purely technical to the multidimensional discipline and identifies thirteen closely interdependent dimensions of InfoSec:

1. The Strategic/Corporate Governance Dimension;
2. The Governance/Organisational Dimension;
3. The Policy Dimension;
4. The Best Practice Dimension;
5. The Ethical Dimension;
6. The Certification Dimension;
7. The Legal Dimension;
8. The Insurance Dimension;
9. The Personnel/Human Dimension;
10. The Awareness Dimension;
11. The Technical Dimension;
12. The Measurement/Metrics (Compliance monitoring/Real time IT audit) Dimension;
13. The Audit Dimension.

According to Von Solms [47], the dynamic nature of InfoSec does not allow one to create a complete list of InfoSec dimensions at any given time. Despite the constant change of dimensions of

the discipline the identification of different dimensions is desired because it will lead to the structuring of InfoSec complexity. Furthermore, only through addressing all InfoSec dimensions in a holistic manner could an organisation develop a secure environment.

The list of the InfoSec dimensions proposed by Von Solms [47] may be extended with the following dimensions derived from the comparative analysis of [72, 235]:

1. The Physical Security Dimension;
2. The System Development Dimension which ensures that the security is built into the development process;
3. The Security Architecture Dimension;
4. The Business Continuity Dimension;
5. The Privacy Dimension.

Blakley et al. [151] refers to InfoSec as a management of risks associated with information and claims that the ultimate task of InfoSec is the determination of the effectiveness of security countermeasures. This attitude to InfoSec was later captured in the term IA (see Section 3 for the detailed discussion.) Blakley et al. [151] points out two reasons of the majority of security failures: (1) limited focus of the discipline (InfoSec generally concerned with technical and logical security countermeasures), and (2) ineffectiveness of security countermeasures. The first reason clearly testifies for a need in diversified solutions for security problems.

The shift of InfoSec from the technical to the broad, multidimensional discipline is also supported by Lacey [46], who recounts that InfoSec "*draws on a range of different disciplines: computer science, communications, criminology, law, marketing, mathematics and more*". Lacey [46] confirms the importance of technologies for protection of information, but emphasises even greater importance of the human factor which is based on the fact that all technologies are designed, implemented and operated by people. In addition to the human factor, Lacey also considers how organisational culture and politics affect InfoSec. Addressing the growing interconnectivity, Lacey [46] gives an account of a recent Internet Age phenomenon - *de-perimeterisation*. De-perimeterisation refers to the erosion of the hard perimeter of an organisation in order to leverage achievement of business goals. Lacey [46] points out an important switch in InfoSec from the protection of isolated enterprise systems to the protection of systems with open corporate boundaries.

De-perimeterisation is also intensively discussed by the Jericho Forum (JF) - the international IT security association, that aims to develop solutions for secure business IT operations. According to the JF, de-perimeterisation is a result of *"a huge explosion in business collaboration and commerce on the Web"* [210]. The JF Commandments state that de-perimeterisation *"has happened, is happening, and is inevitable"* [211] and provide a set of principles to be used for achievement of a *"good security"* in a collaborative, networked world. Although the JF follows a business-oriented approach, it still has a very technical standpoint and concentrates primarily on technical solutions of the issues related to de-perimeterisation (e.g. authentication and authorisation) [211]. Albeit de-perimeterisation is a recent phenomenon, a significant research already exists about the technical solutions that may be used for information protection in the de-perimeterised environment. Nevertheless, for the dimensions of InfoSec other than technical one, the effect of de-perimeterisation is not thoroughly investigated [54].

Thus, at the time of massive interconnection and collaborative information sharing, InfoSec becomes more challenging since information now needs protection not only within the safe organisation's perimeter, but also outside it. This important change within the InfoSec domain is outlined in [41, 42, 54, 46, 210, 211].

The multidimensional nature and the broadening scope of InfoSec is also supported by Dlamini et al. [1] who states that in the first decade of the XXI century three areas became important for InfoSec: legal and regulatory compliance, risk management and information security management. As a consequence, the number of people involved in InfoSec is increasing. If previously there were only technical experts involved in InfoSec, at present managers, legal personnel, compliance regulators, human resources specialists are also involved in InfoSec.

In agreement with other authors, Tiller [43] states the omnipresent nature of InfoSec and, most importantly, proclaims that in addition to a comprehensive approach InfoSec is required to be agile and adaptable to meet the requirements of continuously evolving business needs. The flexible adaptable nature of InfoSec, shown by many authors [42, 43, 47], should be seen as a need to revise the approach to InfoSec as well its definition and its scope on the regular basis.

At the end of the XX and in the beginning of the XXI century a number of documents emerged escalating the importance of corporate governance: the Turnbull Guidance *"Internal Control: Guidance for Directors on the Combined Code"*, the American Institute of Certified Public Accountants (AICIPA) standards, the King report on Corporate Governance, the Organisation for Economic Co-operation and Development (OECD) Principles of Corporate Governance, the 8th audit directive

of the European Union and the Sarbanes-Oxley Act. These documents attracted the attention of senior management to InfoSec problems that were previously deemed to be low level activities and the responsibility of technical personnel. The growing dependence of business on the IT systems led to the importance of InfoSec being recognised at the managerial level. This is depicted in many academic publications where InfoSec, among other dimensions, includes the governance, administration or management dimensions [1, 41, 47, 49].

The analysis of the literature shows that there is a paradigm shift in InfoSec towards a coherent approach to information protection. Previously, the basic assumption was that the technology could provide *"absolute security"* [1]. Nowadays, it is clear that the technology alone is insufficient for solving complex tasks of the discipline. Business needs, the human factor, economic incentives, cultural and organisational aspects should be taken into account in order to achieve an adequate protection of information. At present a comprehensive, multidimensional approach to the protection of information is required.

2.2 Information Assurance

Information Assurance (IA) is quite a new discipline, perhaps, the most striking feature of which is that everyone seems to have different opinion about what it actually is. In order to identify the scope and to understand the meaning of IA, in this section we follow the procedure similar to the one used to analyse InfoSec. First, the understanding of the term based on common English is examined. Then, we present the analysis of the definitions of IA provided by the official organisations, followed by the analysis of the comprehension of the discipline in the academic and industry publications. Finally, an adapted definition of IA is presented.

2.2.1 Common English

For the purpose of working out the general definition of IA, we begin with the definition of the word assurance in the [40]:

- Assurance n.

  1. a positive declaration intended to give confidence; a promise;

  2. confidence or certainty in one's own abilities.

Confidence is defined as "*the feeling or belief that one can have faith in or rely on someone or something*" [40]. Based on the *"distilled knowledge and wisdom embodied in the dictionary definitions"* [41] we coin a general definition of IA:

Information Assurance is a discipline the main aim of which is to give confidence or certainty in information; to give belief that one can rely on data, knowledge, facts, and its meaning.

One important assumption that comes out of the above definition is that confidence in information must be based on confidence in all entities involved in the processes of information processing, storage and transmission. An entity, in this context, may mean a technical tool or system, a process, an individual or an organisation.

Similarly to the general definition of InfoSec, the definition of IA identifies a broad scope of the discipline. In this case, the general definition leaves a plethora of questions for discussion, for example:

- What are the properties that information should have in order for one to be able to rely on it?
- What actions should be undertaken on order to give confidence in information?
- What evidence is required to ensure confidence in information?

In order to find the answers for the above questions, in Section 2.2.2 we analyse the definitions of IA suggested in the official sources.

2.2.2 Official Documents

The term IA was coined by the US Joint Staff in 1998 and for the first time appears in Joint Doctrine for Information Operations [212]. This document provided the classical definition of IA that for the first time declared five security goals, also known as the Five Pillars of IA: availability, integrity, authentication, confidentiality and non-repudiation.

In 2000, the term IA was included into the US National Information Systems Security Glossary, published by The National Security Telecommunications and Information Systems Security Committee (NSTISSC), which in 2001 was given a new name the Committee on National Security Systems (CNSS). Over the decade the definition has changed so that the latest definition refers to

measures, rather than information operations as in the original definition. Below is the definition of IA extracted from the CNSSI [56]:

Information Assurance - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

For the purposes of this definition, the following meanings also apply:

- Availability - The property of being accessible and useable upon demand by an authorized entity.
- Integrity - The property whereby an entity has not been modified in an unauthorized manner.
- Authentication - The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.
- Confidentiality - The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.
- Non-repudiation - Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

This original CNSS definition, based on the Five Pillars, remains the only rigorous definition of IA until present and, therefore, is highly cited. The analysis of the CNSS definition of IA is presented below. First, according to the CNSSI the scope of IA, in terms of security goals, is wider than the scope of InfoSec defined in the same document. In addition to the three security goals of InfoSec - confidentiality, integrity and availability - IA also aims to achieve authentication and non-repudiation. Second, the definition includes in the scope of IA not only information, but also explicitly states an information system as an object for control. The second sentence of the definition is particularly oriented on information systems and gives a technical sense to IA. Third, the Five Pillars of IA present an amalgamation of security goals and security mechanisms. Whereas, *non-repudiation* is another security goal that aims to achieve a state where none of the entities may deny participation in the transaction, *authentication* is a security mechanism that helps to achieve such security goals as confidentiality, integrity and non-repudiation through the

identity verification. The fact that security mechanisms are mixed in the definition with security goals is confusing. Adding to the confusion is the concentration on a certain security mechanism - authentication - and ignorance of other non-less important security mechanisms, e.g. authorisation and cryptography.

The CNSS definition of IA declares security goals, but does not define any methods to be used to achieve them. The clarification on that regard is found in [53, 236] which explain that IA may be achieved *"through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare."* The defense-in-depth concept was adopted by the US DoD from the Information Assurance Technical Framework (IATF) and is based on the long-existing military principle of multilayered protection of fortifications [270, p.39]. As a result of the adoption of the defense-in-depth concept, IA includes into its realm such aspects as [236]:

- Risk management;
- Training, education and professionalism of the staff;
- Program, issue-specific and system-specific policies;
- Monitoring, management and administration;
- Assessment and audit.

In order to understand the concept of IA accepted by the UK government we examined *A National Information Assurance Strategy* that was published by the Cabinet Office in 2007 and the related documents. The glossary of *A National Information Assurance Strategy* [62] defines IA as follows: *Information Assurance is the confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users.*

According to this definition, IA has a very narrow scope and concerned only with the security of information systems. *HMG Security Policy Framework* [218], published by the Cabinet Office, also follows a similarly narrow approach to IA, and concentrates on the risks associated with confidentiality, integrity and availability of information within an information system. IA here has a purely technical interpretation. A detailed analysis of *A National Information Assurance Strategy* shows that this document, in defining IA, puts a strong emphasis on the management of risks to information. That is derived from a definition of IA given in [62, Foreword]: *"Information*

Assurance is the term given to management of risk to information. Effective IA ensures that the opportunities provided by new technology can be exploited to maximum benefit." Further in the text [62] inconsistently refers to the Five Pillars (rather than to the CIA-triad that is stated in the definition of IA provided in the glossary of the same document) and includes information in the scope of IA as well as information systems: *"The term 'information assurance' (IA) is used to describe confidence in the processes of information risk management. Effective IA should ensure appropriate levels of availability, integrity, confidentiality, non-repudiation and authentication of information and information systems."*

In fact, industry response to the IA strategy indicated that the key priorities of the strategy are not obvious and *"clouded by inconsistencies in delivery, belief or understanding."* [70]

In contrast with [62, 218], the *HMG Information Assurance Maturity Model and Assessment Framework* [213], proclaims a broader viewpoint on IA. It considers IA as a systematic, business enabling and dynamic approach to InfoSec which is not limited purely to information systems. According to [213], the IA scope is much wider than the scope defined in [62] and comprise a diverse range of aspects including: leadership and governance; training, education and awareness; information risk management; through-life IA measures; assured information sharing; and compliance.

Albeit the uncertainty with the interpretation of IA in the UK official sources, it is clear that the perception of IA has a pronounced tendency towards technologies and information systems, and is focused on the management of risks to information, primarily associated with information systems. This is clearly declared in the vision of the *UK National IA strategy* for 2011 [62]: *"A UK environment where citizens, businesses and government use and enjoy the full benefits of information systems with confidence."*

Finally, according to the official sources, IA is concerned with a coherent multilayered protection of information. It is worth noting that the documents concentrate on protection of information in electronic form circulating within computer systems and networks. The aspects such as risk assessment, monitoring and management are included in the scope of IA as a way of achieving a fair balance between security controls in the three layers of protection.

2.2.3 Academic and Industry publications

Since 1998, when the term IA was coined by the US military agencies, researchers and industry have been showing constant interest in IA. Although IA has existed for more than ten years, there is still no commonly agree understanding of it in the literature. In 2002, Kovacich stated: *"Information Assurance is one of the newly refined processes of information protection that has evolved from computer security and information system security. Is it InfoSec by another name, a subset, or just the other way around? There is some argument about that."* [270, Foreword]. This argument is still valid today. In this section, delving deeper into the meaning of IA, we examine the perception of IA in academic and industry publications.

At the time when IA emerged, the environment was changing in two directions simultaneously: first, the world was getting more interconnected and, second, the importance of InfoSec was recognised at the managerial level (Section 2.1.3). Consequently, IA, which was deemed to address the change of the environment, received several interpretations, and, as a result, the focus and goals of the new discipline are noticeably inconsistent in various sources. The analysis of the related publications has identified three divergent interpretations of IA:

1. IA as a discipline dealing with the technical network-related security issues;
2. IA as a process of establishing confidence in information and information systems;
3. IA as a comprehensive management of InfoSec.

The third interpretation is the broadest one and is widely inclusive. It includes the technical aspect of IA, dominating in the first approach, and the establishment of confidence in information and information systems, dominating in the second approach. In some publications, an amalgamation of the approaches could be found. Nevertheless, in most cases the publication places a clear emphasis in its approach to IA which allows us to ascribed the work precisely to one of the three approaches. The approaches to IA listed above are outlined in detail in the following three sections.

2.2.3.1 Information Assurance as a discipline dealing with the technical network-related security issues

This interpretation is reflecting the change of the environment in terms of the growing interconnectivity and is solidly based on the original definition of IA, proposed by the US military agencies.

IA here is considered as a subset of InfoSec, focusing on the network security. The Five Pillars (confidentiality, integrity, availability, authentication and non-repudiation) are the goals of the discipline. This approach was prevailing in the late 1990s and the early 2000s. It was and still is mainly supported by technical security specialists and government agencies.

The technical orientation implies that the discipline focuses on security of information systems and information within information systems. Consequently, security goals here describe the desirable properties of information systems, rather than properties of information. This, possibly, explains the fact that authentication, which is, in fact, a security mechanism, is included in the list of security goals.

In 2001, Maconachy et al. [86] presented a model of IA. IA according to Maconachy et al. is the next step of the InfoSec evolution. The model is an extension of the InfoSec model, originally proposed by McCumber [65], where the CIA-triad is replaced with the Five Pillars. Maconachy et al. [86] adopts a comprehensive and multidimensional approach to IA which stems from the defense-in-depth concept, but the goals of the discipline in this work are still limited to Five Pillars.

In 2002, McKnight [107] defined IA from a purely technical viewpoint. Importantly, McKnight [107] acknowledges that none individual viewpoint (including the technical one) would allow the creation of a correct picture of the discipline. Thus, the author recognises that IA extends beyond the technical domain. McKnight [107] further states that in a broad sense IA incorporates the product, procedures, and policies that allow the timely transfer of information in an accurate and secure way among involved parties. McKnight [107] claims that InfoSec is not the same discipline as IA, but does not discuss the distinctions between the disciplines. The author claims that technology and policies may change over time, whereas security goals will remain persistent. This claim is only partially true: although previously defined security goals (confidentiality, integrity, availability) stay consistent, the new security goals constantly evolve to reflect new threats. This issue is discussed in more detail in Section 2.1.

2.2.3.2 Information Assurance as a process of establishing confidence in information and information systems

This approach is based on a common understanding of the term *assurance* and correlates with the general definition of IA derived in Section 2.2.1. Here, IA is not an independent discipline, but an InfoSec subset which deals with (1) the classification of information by the level of confidence one

may have in it or by correctness of information [42] and (2) the evaluation of the system's level of security [49].

In order to establish confidence in an information system, one needs to have an up-to-date model of evaluation criteria, as well as unambiguous security metrics and an agreed evaluation procedure. The Common Criteria for a long time has been serving as a model of evaluation criteria. This approach is clearly oriented on the evaluation and demonstration of the security level in order to gain trust of the internal and external parties (stakeholders, users, authorities, partners, customers etc.)

2.2.3.3 Information Assurance as a comprehensive management of Information Security

This interpretation reflects the recognition of the importance of InfoSec for business success and a need to address it at the managerial level. A certain element of *fashion* plays its role in the use of the term IA in this context. This approach to IA emerged in the early years of the XXI century and is widely adopted by the commercial world. The origins of this approach are rooted in the defense-in-depth concept. Here, IA is interpreted as comprehensive and systematic InfoSec management. The main aim of IA is not the achievement of pre-defined security goals, but the successful business operation and the overall protection of information [71]. This approach may be considered as an extension to the original concept of IA proposed by the DoD where IA is taken from the technical level, considering protection of information in the networked computerised systems, to the managerial level, concerned with the protection of business in the interconnected world.

This approach more than any other correlates with the general definition developed in Section 2.2.1, because only the comprehensive and systematic management of information and information systems may provide a sought-for confidence in information. In this approach technology is not the primary focus of the successful information protection. Here, InfoSec is deemed to be either a subset of IA or a concomitant discipline.

In 2002, the Information Assurance Advisory Council (IAAC), a UK-based not-for-profit research organisation, in association with Microsoft published *"Benchmarking Information Assurance"* [71]. This document most prominently illustrates the discussed approach to IA. This document presents public and industry point of view on IA, and supports the argument about the little agree-

ment on the concept and terminology related to IA. The IAAC states that the terms InfoSec and IT security over-emphasise the importance of confidentiality and miss out other problems such as accessibility or reliability, whereas IA overcomes these issues. Furthermore, the emphasis put on IT, also means that the risk to information is seen as a low-level activity, which is outside of the interests of senior management [71]. The survey conducted by the IAAC demonstrated that IA attracts more and more attention of top managers across multiple sectors, but more rapidly an integrated approach to information protection is accepted by smaller organisations.

Thus, the IAAC considers IA to be an activity dealt with at a higher level than InfoSec. InfoSec is a responsibility of computer specialists, whereas IA is a responsibility of senior management. IA is the systematic management of InfoSec, based on a holistic strategy. This also confirmed by the fact that BS7799 *Information security management. Code of practice for information security management systems* is considered to be the foundation of IA [71]. Interestingly, neither BS7799, nor the ISO/IEC 27000 series use the term IA or provide a definition of it. Nevertheless, other works (e.g. [71]) refer to BS7799 and the ISO/IEC 27000 series as the IA standards, confirming the understanding of IA as a management of InfoSec.

Boyce and Jennings [270] explain the concept of IA as it may be applied in the private and public sectors. The authors define IA as *"the process for protecting and defending information by ensuring its confidentiality, integrity, and availability. At its most fundamental level, IA involves protecting the rights of people and organisations."* Boyce and Jennings discern two main functions provided by IA: (1) the protection of an organisation's own rights (rights to survive, coexist and grow) and (2) the protection of other parties that interact with an organisation. The approach to IA presented in [270] spreads through both technical and managerial perspectives. The authors point out that at present, when technology is at the very core of any business, IA becomes an indispensable component of overall business performance. In terms of the goals of the discipline Boyce and Jennings, in addition to the CIA-triad also in detail discuss auditability (the ability to verify the activity of a security control), accountability (holding of individuals liable for certain activities), access control, risk management, cost effectiveness, comprehensive and integrated approach, life-cycle managements, training and awareness, and continual reassessment. Although the authors still consider in detail the technical side of IA, they place the main emphasis on the importance of addressing information protection in the networked environment at the managerial level. Boyce and Jennings [270] highlight that IA, by protecting information, a *"critical and strategic business resource"*, supports the mission of an organisation.

Tawileh and McIntosh [214] also perceive IA as a separate discipline and the next step of the evolution of InfoSec, which in the process of its development and expansion, includes new aspects. The shift from InfoSec towards IA stems from "*the changes in the organisational environments and the information systems developed to serve these organisations*" [214] when in addition to the technological solutions, human and organisational aspects began to be taken into account.

The analysis of the literature shows that the commercial sector eagerly adopted the defense-in-depth concept which serves as the kernel of IA. The commercial world rather than to concentrate on the technical side of network protection and on the Five Pillars of IA, preferred to focus on the essence of IA - the comprehensive and systematic management of InfoSec based on the utilisation of a reasonable combination of the capabilities of people, operations and technology.

In 2011, as a part of this PhD project a survey was conducted among one hundred of InfoSec and IA professionals. One of the aims of the survey was to identify the most commonly accepted perception of IA. The survey showed that the largest group of respondents (45 out of 100) is inclined to understand IA as a holistic, multidisciplinary and systematic approach to InfoSec. This approach corresponds with the interpretation of IA as a comprehensive management of InfoSec as outlined in this subsection. The full results of the survey are presented in [32].

2.3 Adapted Definitions of InfoSec and IA

Albeit that, at the first glance, the meaning of InfoSec is fairly intuitive, the scope and the goals of the discipline are ambiguous. The analysis undertaken shows that the lack of an agreed definition and an unclear scope of InfoSec are the problems troubling the discipline. Until now, nobody seems to have produced a single, all-encompassing definition of InfoSec, possibly due to the complexity and persistent alteration of the discipline. The definitions provided in the standards are not adequate and do not reflect the broad scope of the discipline described by the academic and professionals (Section 2.1.2). We have not found a clear rigorous definition of InfoSec in either the academic or industry publications (Section 2.1.3). Some of the definitions of InfoSec found in academic publications are listed in Table 2.4.

The examination of the term IA, based on the analysis of the standards, academic and industry publications, confirmed that IA has various interpretations. IA was originated in the US military agencies as a discipline dealing with the technical security issues in the new networked environment. Later, the defense-in-depth concept, which lies at the very heart of IA, was taken up by

Table 2.4: The Existing Definitions of Information Security

Source	Definition of Information Security
[42]	Information Security is the process of protecting the intellectual property of an organisation.
[151]	...information security is a risk management discipline, whose job is to manage the cost of information risk to the business.
[223]	A well-informed sense of assurance that information risks and controls are in balance.
[225]	Information security is the protection of information and minimises the risk of exposing information to unauthorised parties.
[72]	Rather than being a separate study, information security draws from a number of other academic domains. These include: computer science, computer architecture, forensics, cryptography, knowledge and information theory, business, mathematics, military science, law and ethics, software engineering, statistics and all things having to do with the Internet.
[41]	Information security is the enabling technology of electronic business [p.5]. Information systems security is only a small part of information security, which in turn is but one part of a wider topic: business assurance [p.24].
[1]	Information security has evolved from addressing minor and harmless security breaches to managing those with a huge impact on organisations' economic growth. ... Does this mean information security is a new field or just another "fad"? No, information security is neither new nor a "fad". What is new is its broader focus and wider appeal.
[73]	Information Security is a discipline governing the framework for the continuous cycle of safeguarding information and ensuring related regulatory compliance.
[74]	Information security is not just a technical issue, but a very important management issue, its main purpose is to create a secure information environment.
[28]	Information Security, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology. [p.8]
[215]	Information security is the assurance and reality that information systems can operate as intended in a hostile environment. [p.8]

the commercial world and intensively supplemented with the new findings. At the turn of the century, the commercial sector recognised a need for a comprehensive and systematic approach to managing InfoSec. IA, which was coined at the same time, was deemed to be a modern response to that growing need. As a result, IA transformed from a discipline dealing with the exploitation of people, operations and technology capabilities in order to protect information in the networks to the discipline of a comprehensive and systematic management of InfoSec needed in order to improve overall business security and productivity. Thus, over the last decade IA evolved from the technical discipline dealing with the network security issues into the broad discipline which now includes soft aspects like administration, training and education.

Further, research has showed that, at present, there is no definition of IA which reflects the discipline in its broadest sense. The original definition of IA, based on Five Pillars, does not reflect the complexity and scope of the discipline in full. Similarly with the definitions of InfoSec, the definition based on a certain set of security goals has become obsolete very rapidly in the current changing environment. Moreover, the definition based on the Five Pillars limits not only the goals of the discipline, but also security mechanisms that may be used. The evolving nature of the discipline and its broad scope should be captured in the definition. Ideally, the relationship between InfoSec and IA should be clarified.

In order to summarise the enhanced understanding of the burgeoning areas of InfoSec and IA, and to address the drawbacks of the existing definition, we endavour to develop the adapted contemporary definitions of the disciplines. The definitions, by no means, attempt to introduce new knowledge or concepts. They only attempt to synthesise and express in a concise form the outcomes of a thorough analysis of the security-related literature presented in the previous sections. Below we present a two-part adapted definition of InfoSec and an adapted definition of IA:

Information Security *is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security countermeasures of all available types (technical, organisational, human-oriented and legal) in order to keep information in all its locations (within and outside the organisation's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destructed, free from threats.*

Threats to information and information systems may be categorised and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with

the evolving environment. The currently relevant set of security goals may include: confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability.

***Information Assurance** is a multidisciplinary area of study and professional activity which aims to protect business by reducing risks associated with information and information systems by means of a comprehensive and systematic management of security countermeasures, which is driven by risk analysis and cost-effectiveness.*

This section concludes by reviewing the advantages of the elaborated definitions. The advantages of the proposed two-part definition of InfoSec:

- The definitions explicitly reflects the multidisciplinary nature and the diverse scope of InfoSec in its current reincarnation (1) by declaring a wide range of security mechanism that could be exploited for information protection and (2) by outlining an extensive list of security goals which will be justified in Chapters 3 and 4.
- The definition puts the correct emphasis among the priorities of InfoSec by stating the protection of information from threats as a primary goal of InfoSec and protection of information systems as a consequent goal.
- The definition clearly distinguishes security goals from security countermeasures which may be exploited in order to achieve security goals.
- The definition distinguishes four types of security mechanisms:

    1. *Technical* (e.g. biometrics, firewalls, PKI, digital signature, malicious code, virus and intrusions detection systems etc.)
    2. *Organisational* (e.g. strategy, policies, processes, audit, physical security, recovery plans etc.)
    3. *Human-oriented* (e.g. training, education, motivation, ethics, culture etc.)
    4. *Legal* (e.g. legislation, Job contracts, non-disclosure agreements, service-level agreements,)

    The lists of security mechanisms within each type is by no means exhaustive and only intended to give an idea of a variety of security mechanisms available.

- Following the traditional approach to defining InfoSec, the proposed definition refers to security goals. J. Anderson [223] states that the definition of InfoSec should provide more guidance about the objectives of InfoSec programs. In addition to naming security goals, the second part of the definition explains the origins of security goals. This information is essential for understanding, particularly, for newcomers to the field, but omitted in all known to us definitions of InfoSec.

- Although the definition outlines the currently relevant set of security goals, it does not limit the scope of InfoSec to the listed goals. The refined definition leaves the space for the natural changeability of the discipline and for open-mindedness among security experts by declaring a need of a regular revision of security goals.

- The definition reflects the growing trend in InfoSec towards the open, de-perimeterised environment by pointing out the need to protect information outside an organisation's perimeter as well as inside it.

The advantages of the proposed definition of IA:

- Importantly, the definition of IA declares the protection of a business as the ultimate goal. Although the security goals of InfoSec are inherited by IA, since IA has a wider scope and incorporates InfoSec, it is important to outline in the definition of IA that the reason behind all IA activities is the overall protection of business.

- The definition declares a need in a comprehensive and systematic management of security countermeasures. *Comprehensive* management means that security mechanisms of all available types should be exploited, the scope should not be limited to technical mechanisms. *Systematic* management refers to the fact that information protection should be addressed consistently at every stage of the system life-cycle.

- The definition declares two main drivers behind security decisions:

  Risk analysis - IA does not attempt to eliminate all risks, the risks should be prioritised, according to the organisation's specifics, and reduced to an acceptable level;

  Cost-effectiveness - IA does not attempt to achieve security at any price, but in a most efficient and cost-effective way.

- The suggested definition clarifies the relationship between InfoSec and IA. If InfoSec is concerned with the development and implementation of security mechanisms, IA is con-

cerned with the design of a sensible and effective combination of security countermeasures. In short words, it is possible to say that IA is a comprehensive and systematic management of InfoSec.

The proposed definitions were developed by the author of the thesis based on the extensive analysis of the IAS literature as demonstrated above. The analysed literature includes official standards, academic and industry publications. This analysis is also presented in [7].

According to the Definitions 1 and 2, InfoSec deals with the development and implementation of security countermeasures, while IA is a management of InfoSec. The border between InfoSec and IA is very vague and the overlap is substantial. In this research, the joint domain of IAS is addressed. The IAS domain incorporates knowledge of both InfoSec and IA. (Since 2005, the term IAS has been used in US to label the area of knowledge, covering security in IT education programs [8].) Thus, in the scope of IAS this includes all actions directed at keeping information secure as well as the management of these actions.

2.4 Trends in the Evolution of IAS

Summarising the findings regarding the scope and the current state of IAS, the following trends in the recent evolution of IAS were identified [7]:

1. The approach to information protection for a long time has been primarily focused on technical solutions of security issues. The protection of information systems and networks is certainly important, but represents only one facet of the problem. The IAS literature analysis demonstrates that there is a paradigm shift in IAS towards an holistic approach to information protection. In order to achieve adequate security the full spectrum of issues related to information protection should be addressed. Business needs, the human factor, economic incentives, cultural and organisational aspects should be taken into account in order to achieve adequate protection. In response to this, IAS adopts an holistic, multidisciplinary and systematic approach to information protection. IAS has moved from a low-level technical activity and responsibility of computer specialists to a top priority activity dealt with at the strategic managerial level [1]. Moreover, IAS is recognised as an integral part of business and a business enabler [41].

2. IAS has become a much-diversified multi-disciplinary field of research and practice. The aspects related to management [41, 42, 43], marketing [41], economics [44, 45], physiology [45, 46], law [46, 47], sociology [48], criminology [46, 48], mathematics [46, 49] and other disciplines are now considered to be in the scope of IAS. Currently, IAS has a broad scope, and requires knowledge of experts in different disciplines.

3. IAS shifts from the protection of “closed" Information Systems (ISs) to the protection of open systems operating in a collaborative interconnected environment [7, 41, 42, 50, 54]. Organisations intensively collaborate - share information, integrate ISs and business processes. E-commerce, outsourcing and cloud computing assume information sharing with external parties and induce a proliferation of inter-organisational dependencies. In this landscape, IAS becomes more challenging because information needs protection, not only within the safe boundaries of an organisation, but also outside of them - in the outer world, where an organisation has little or no control over its information.

4. *"Information exists both inside and outside the computer and has to be protected wherever it travels"* [42, p.13]. The scope of IAS shall not be restricted to protection of information within computer systems only. From the IAS perspective, information in any form (electronic, paper, knowledge (verbal) etc.) requires protection.

2.5 Security Goals as One of the Key Concepts of IAS

The literature analysis, which is presented in the previous sections and in [7], confirms that security goals play an important role in the IAS domain. The analysis shows that, traditionally, InfoSec and IA are defined via a set of security goals (e.g. in standards such as ISO/IEC 27000 [55], CNSSI [56] and ISACA [57]). The majority of conceptual models of IAS include security goals as discussed later in this chapter. The identification of security goals is one of the initial steps in various risk management approaches [58, 59]. In Process-Aware Information Systems security configurations, legal regulations and risk assessment are expressed via security goals [60].

A security goal corresponds to and reflects the protection of information from a certain category of threats [61]. For instance, confidentiality refers to a desirable ability of an information system to prevent an unauthorised access to information. All threats that may be categorised as an unauthorised modification of information are grouped in and addressed by the concept of integrity. All threats that may result in a denial of service are captured in the concept of availability.

Since the late 1970s, InfoSec has been rigorously associated with the classic information security triad - confidentiality, integrity and availability (also referred to as the CIA-triad) [28]. The members of the CIA-triad and other security related properties of information and an IS are interchangeably referred to in the literature as security attributes, properties [62, 56], goals [208], fundamental aspects [42], information criteria [64], critical information characteristics [65] and basic building blocks [42]. In order to highlight the fact that these are the *desirable* properties of information or *desirable* abilities of an IS, where appropriate, in this thesis the term *security goal* is used to refer to confidentiality, integrity, availability, non-repudiation, accountability, privacy, auditability, authenticity and trustworthiness. In this thesis, a distinction is made between a *security goal* and a *security countermeasure*. A security countermeasure is defined as a technique or a process by which a certain security goal(s) is achieved. While a security goal identifies “WHAT" in terms of security should be achieved, a security countermeasure refers to “HOW" it should be achieved.

The literature analysis confirms that, in recent years, there is a pronounced tendency to extend the scope of IAS beyond the CIA-triad since the latter is found to be no longer adequate because it does not cover newly emerging treats to information (e.g. social engineering) [28, 66]. A plethora of security goals is considered to be relevant to IAS and is intensively discussed in the literature. A large number of publications was analysed in order to identify what security goals are associated with IAS:

- Table 2.2 analyses security goals addressed in the IAS publications;
- Table 2.7 lists security goals included in the existing conceptual models of IAS; and
- Table 5.5 in Chapter 5 examines security goals considered in the system engineering literature.

All three tables, the latter two of which are discussed in greater detail later in the thesis, evidence that the range of security goals which authors assign to IAS vary from publication to publication, and depends on the author’s background and approach to security. The analysed publications rarely provide any justification for a set of declared security goals. The set of goals is typically drawn upon the author’s practical experience (e.g. in [66, 67])

Summarising the analysis of the literature regarding security goals, two inferences are drawn. First, the concept of a security goal is one of the central concepts in IAS. Second, authors associate a

broad range of security goals beyond the CIA-triad with IAS, but there is no one widely-accepted list of security goals.

The analysis of security goals is continued in Section 2.8, where security goals included in the existing conceptual models are examined.

2.6 Importance of a Conceptual Model of IAS

IAS, as with any area of research and practice, requires precise structuring and formalisation. As often acknowledged, many security issues are caused by wrong security decisions taken on the basis of incomplete knowledge or misunderstanding of the security domain: threats, security goals and available countermeasures [68]. In order to overcome this issue, the main entities of the knowledge area as well as the relationship between them should be defined and brought together in a conceptual model.

A conceptual model of the IAS domain structures the acquired body of knowledge, creates a common ground for InfoSec and IA professionals, and serves as a conceptual framework and a theoretical background for the researchers. A model clearly visualises the IAS domain and enables newcomers to get a quick appreciation of its diverse and complex nature. It assists in informing non-technical and non-security experts about the IAS domain. A descriptive and holistic model encourages the creation of a common language allowing security and business experts to communicate more effectively [50]. It helps practitioners to do their job more effectively by fostering a profound, systematic understanding of the IAS domain that they can also share with the wider business community.

A conceptual or reference model of IAS plays a crucial role in the context of an IS as it serves as a blueprint for the design of a secure IS. It provides a basis for the elicitation of system security requirements and for the development of an Information Security Policy Document (ISPD) [69, Sec.5]. The model may be used for tracing security vulnerabilities and for security benchmarking [65].

2.7 Need for a Regular Revision of an IAS Conceptual Model

IAS is a constantly developing domain, which changes shape following the evolution of society, business needs and ICT. Many studies highlight continual changes of IAS [42, 46, 49, 50, 66]. A conceptual model of a discipline often becomes debatable and requires a revision when the area of knowledge evolves and broadens [33]. Therefore, the conceptual model of IAS should be revised regularly to reflect the changes in the domain [66, p.228],[61].

As IAS evolves a conceptual model of the domain must be revised and updated in order to capture and adequately reflect the meaning and scope of IAS in its current state. Thus, the trends in the evolution of IAS which are summarised in Section 2.4 must be reflected by a model of the IAS domain.

Finally, the analysis of literature with regard to security goals confirms (1) a set of security goals must be included in a conceptual model of IAS as the notion of security goals is crucial for the domain, and (2) a list of security goals included in a conceptual model must be thoroughly elaborated.

2.8 Critical Analysis of the Existing Models of IAS

Until the 1990s, InfoSec was described by access control and information flow models (e.g. [75, 76, 77, 78]). These mathematical models were followed in time by conceptual models which attempted to cover the full breadth and heterogeneity of InfoSec. The purpose of a conceptual model of IAS is to convey the complexity of the domain to a management team and later on to a wider non-technical audience.

Initially, this section describes the systematic literature review methodology exploited. Then, the section contains an overview of seventeen conceptual models and frameworks of InfoSec and IA. Finally, this section considers the advantages and drawbacks of the analysed model.

2.8.1 Literature Review Methodology

A systematic review of the proposed models/frameworks of InfoSec and IA was conducted following the methodology suggested in [79] where it is used for the analysis of security ontologies. This methodology ensures that all papers, which are relevant to the subject of a research, are captured and that the important information from the selected papers is consistently extracted.

The review was expected to answer the following questions: *What models/frameworks were proposed to capture the knowledge of InfoSec and IA?*, *What IAS concepts are included in the models/frameworks and why?*, *How are they represented visually?*, *How are they evaluated, validated?* and *What are the advantages and drawbacks of the existing models?*

Two groups of representative keywords were identified and used in combination for the discovery of the relevant proposals. The first group is "Model, Conceptual Model, Reference Model, Framework"[1]. The second group is "Information Security, Information Assurance, Information Security Management". The keywords from both groups were combined in a search query. The search was conducted in the following sources: Google Scholar, ACM Digital Library, IEEE Xplore Digital Library and SCOPUS. The search was also performed in Google Search Engine to ensure that not only academic proposals, but also proposals from industry and practitioners are included in the analysis. After the primary proposals were selected from the searches, the citations in those papers were traced.

At this stage 52 proposals were selected based on the title, keywords and abstract (or full text, where immediately available). The papers were examined and out of them closely related proposals were selected for the detailed analysis according to the following criteria. A proposal where a model/framework has a visual representation was included, although the absence of a visual representation alone was not a reason for the exclusion. A proposal was selected if it addresses the IAS domain in general. Some domain-specific models (e.g. models for governments and e-business) were also selected as they exploited a comprehensive approach to IAS. Maturity models were excluded from the analysis because rather than describing the domain, they describe various stages of the InfoSec maturity of an organisation. Only papers which are published in English were included in the analysis.

[1]The term "reference model" is comparatively new. Therefore, some examples of the IAS knowledge representation that, according to the modern terminology may be refereed to as reference models, in the original publications are referred to as conceptual models or frameworks.

Finally, seventeen models and frameworks of IAS were selected for the detailed analysis which is presented in the remainder of this sections.

2.8.2 Discussion of the Existing Models

2.8.2.1 The CIA-triad

The CIA-triad (confidentiality, integrity, availability) has been serving as a conceptual model of computer security for several decades and, later, InfoSec [28]. Its origin could be traced back to 1975, when Saltzer and Schroeder [94] stated that at that time security specialists distinguished three categories of threats to information: unauthorised information release (refers to confidentiality); unauthorised information modification (refers to integrity) and unauthorised denial of use (refers to availability). The term CIA-triad, as we know it today, appeared only in 1986-1987. The term was coined in Johnson Space Center, USA [61] and, for the first time, appeared in a JSC-NASA Information Security Plan, also known as "The Pink Book" in 1989. The CIA-triad rapidly gained popularity among InfoSec practitioners. Until now, a wide range of security-related material is based on the CIA-triad, despite the fact that the adequacy of the CIA-triad is questioned [28, 66]. Surprisingly, according to Leo, one of the authors of the CIA-triad, the CIA-triad was not intended to be a precise and comprehensive definition of InfoSec, it was only intended to convey the overarching goals of InfoSec to business and engineering management in a simplified way and in a terminology that will be easy to understand [219]. Despite the original intention, up to now, the CIA-triad has often been mistakenly interpreted as an exhaustive set of technical requirements towards a secure system or as a comprehensive academic definition of InfoSec. This work supports the argument about the incorrectness of adopting the CIA-triad as a complete set of security goals (cf. [28, 66]).

2.8.2.2 McCumber's Cube or CNSS 4011 Security Model (McCumber [65])

The first multi-dimensional model of InfoSec was suggested by McCumber in 1991 [65]. The model (also known as McCumber's Cube) is a part of the National Training Standard for Information Systems Security Professionals (CNSS 4011) [28, p.15].

McCumber's Cube is the first model to promote a comprehensive approach to InfoSec which is not limited to the technological aspect of information protection. McCumber transfers emphasis of In-

foSec from securing IT on to the protection of information. McCumber's Cube may function as an assessment and development framework, and help to identify and mitigate system vulnerabilities. The model consists of three building blocks: (1) Information States (transmission, storage and processing); (2) Critical Information Characteristics (confidentiality, integrity and availability); and (3) Security Measures (technology, policy and practices, and education, training and awareness).

McCumber's Cube has a Rubic's cube shape and forms twenty-seven areas that should be addressed by InfoSec. For example, one of the cubic blocks refers to the policy and practices, which should be in place in order to protect confidentiality of information while it is transmitted.

The comprehensiveness of McCumber's Cube at present is debatable. Other works expand the building blocks of the Cube (e.g. information characteristics [66], security countermeasures [50]) and introduce the new building blocks (e.g. time [86, 93], cost [93]). McCumber's Cube does not explicitly address the protection of information in a collaborative environment and cross-organisational business processes. Despite some drawbacks, until now, McCumber's Cube, may be regarded as the clearest model of InfoSec, which along with the ease of its application explains the fact of its adoption in education.

2.8.2.3 An Integrated Model of Information Assurance (Maconachy et al. [86])

In 2001, Maconachy et al. [86] extended McCumber's Cube. The integrated model of Information Assurance has four dimensions [86]: (1) Information States (Transmission, Storage, Processing); (2) Security Services; (3) Security Countermeasures; and (4) Time.

Maconachy et al. [86] updated McCumber's Cube with the latest findings of that time (1) the list of security services or critical Information characteristics was enriched with non-repudiation and authentication adopted from the definition of IA, and (2) the categorisation of security countermeasures was taken over from the defence-in-depth concept. The model, generally, promoted the holistic approach to InfoSec and was a first attempt to address security issues related to networks. Nevertheless, the set of security goals limited to confidentiality, integrity, availability, authentication and non-repudiation does not reflect the present state of InfoSec and IA. The classification of security countermeasures also requires a refinement.

Maconachy et al. [86] introduce time as the fourth dimension of the model with the purpose of conveying the following aspects: (1) The change of connectivity of a system and, consequently, of risks over time; (2) The need to consider the model at all stages of the ISDLC; and (3) The

learning continuum resulting in an increased level of knowledge and the consequent improvement of InfoSec.

The Maconachy et al. model [86] has been accepted by a group of representatives of fifteen U.S. undergraduate Information Technology programs, IEEE, ACM and ABET as the model of the IAS knowledge area because the model, first, is easy to understand by IT students and, second, is rich enough to tie the IAS domain to other areas of knowledge incorporated in the IT curriculum [8].

2.8.2.4 Parker's Model of Information Security (Parker [66, 61]

In 1998, Parker [66] suggested a new model of InfoSec which consists of six essential foundation elements, also known as the Parkerian Hexad: availability, utility, integrity, authenticity, confidentiality and possession. Parker claims that his model addresses the limitation of InfoSec to the CIA-triad. This limitation is dangerous since the CIA-triad no longer covers all possible violations of security [66].

In 2010, Parker [61] further elaborated his model of InfoSec based on the analysis of security polices of various organisations. Parker's new model incorporates (1) the security states of information (or security goals) that needs to be preserved; (2) the types of acts that induce risk to information; (3) the types of control and practices, and (4) the objectives of InfoSec which may serve as a kernel of security policy of an organisation.

Parker clearly demonstrates that the CIA-triad is no longer adequate as the model of IAS and requires an extension. The value of Parker's model also lies in summarising the practical experience in InfoSec. Among the drawbacks of the model the following may be listed:

- The Parkerian Hexad does not capture some security goals (e.g. privacy, accountability) and, therefore, it needs further elaboration.
- The types of malicious acts that induce risks to information duplicate information conveyed by security goals because each security goal refers to a certain type of security violations, in other words, to a certain type of malicious acts. For example, according to Parker, authenticity covers the misrepresentation of information. Therefore, if the model includes both authenticity as a security goal and misrepresentation as a malicious act it means that information in the model is duplicated because both authenticity and misinterpretation refer to the same concept.

- The classification of controls and practices exploited for information protection is inconsistent. One classification is based on the time of control implementation and its purpose (e.g. prevention, detection, recovery and correction). Other classification is based on the nature of controls (motivation, education, audit sanctions and rewards).

2.8.2.5 Information Assurance Conception Model (Lü [93])

In 2006, Lü [93] proposed an Information Assurance Conception Model which comprises four dimensions: capability, countermeasure, cost and time. The IA countermeasures are split into three groups: technology (access control, audit, security protocols etc), management (risk assessment planning, maintenance etc.) and people (awareness, training, education).

Lü [93] criticises McCumber's Cube for concentrating on information characteristics only and ignoring the characteristics of an information system. Integrity, according to Lü [93], includes the correctness and reliability of an operating system in addition to integrity of information. The difference between authenticity and non-repudiation, as defined by Lü, is not clear since both terms seem to refer to the same characteristic of information (authenticity refers to the confirmation of the data source; non-repudiation refers to providing the proof of data origin). Lü [93], in line with Moconachy et al. [86], considers time as the fourth dimension of IA.

In [93], cost is considered as an important dimension of IA since any organisation is concerned with the increase of the return on security investments. According to Lü [93], IA cost is calculated as a sum of time cost, workforce cost and the cost of software, hardware and maintenance. Lü [93] suggests an abstract formula for comparing IA strategies by cost.

2.8.2.6 Business Model for Information Security

In 2008, ISACA (a non-profit, global association which develops practices for information systems) adopted from the University of Southern California (USA), Marshall School of Business Institute for Critical Information Infrastructure Protection its Systemic Security Management Model. The model since then is named the Business Model for Information Security (BMIS) [50]. The BMIS exploits system thinking in order to structure the complex and dynamic field of InfoSec. The BMIS attempts to tackle the following problems: 1) Changing risk profiles; 2) The lack of a common InfoSec language between management, security experts and other professionals; and 3) The ignorance of InfoSec within organisational culture.

The BMIS consists of four elements: (1) Organisation design and strategy element; (2) People element; (3) Process element; and (4) Technology element. The elements are linked together by six dynamic interconnections: governing, culture, enabling and support, emergence, human factors, and architecture.

ISACA [50] criticises other models of InfoSec as being simplistic, static and not being able to address the changes within enterprise and the culture adaptability, but the source neither presents an analysis of the models nor specifies the models it refers to. In comparison with the other models of InfoSec, such as, for example, McCumber's Cube [65], the BMIS is limited to the consideration of countermeasures only. It does not in any way describe the information which is being protected. The model also does not list the security goals that should be achieved. Several security goals are mentioned in the description of the model (availability, integrity, confidentiality and accountability) [50], but there is no explanation about why these security goals are important or how they may be achieved.

The BMIS describes what components should be in place for InfoSec to be adequate and splits them into elements and interconnections. The difference between elements and interconnections is not explained. For example, it is not clear why an *organisational strategy and design* is an element of the model, while *organisational culture* is an interconnection. The human factor in the BMIS is only considered important in the interactions between people and technology. In this work, the significance of the human factor is considered to be much wider: if people do not understand the organisation's mission or goals, it may cause equally serious issues to the ones caused by people not understanding security technology. Although [50, 220] point out to the importance of addressing inter-organisational information sharing, the BMIS itself does not provide any means for it.

2.8.2.7 Non Risk Assessment Information Security Assurance Model (Al-Hamdani [90])

Al-Hamdani [90] proposes an Information Assurance model based on the diligence approach. The model outlines: (1) security goals (the model adopts the Parkerian Hexad: availability, utility, integrity, and authenticity, confidentiality and possession or control); (2) the classification of data loss (destruction, interference with use, the use of false data, modification or replacement, misrepresentations or repudiation, the misuse or failure to use, disclosure, observation, copying, taking, endangerment); (3) safeguards to protect information (avoidance, deterrence, detection,

prevention, mitigation, transference, investigation, sanctions and rewards, recovery, correction, education); and (4) the layers of protection which are adopted from [270]: policies, management, architecture, operational security administration, configuration management, life cycle security, contingency planning, education, training, and awareness, policy compliance oversight, incident response and reporting.

The shortcomings of the Al-Hamdani model [90] are listed below (some of them are similar to the drawback of Parker's model [61]): (1) the classification of data losses duplicates information conveyed by security goal; (2) the classification of safeguards is inconsistent; (3) the distinction between safeguards and layers is not clear (e.g. education is mentioned both as a safeguard and as a layer); (4) the protection of information outside the organisations' perimeter is not addressed; and (5) information being protected is not described in any way.

2.8.2.8 Information Security Ethics Education Model

Information Security Ethics Education Model, which is tailored to teach InfoSec ethics, is presented in [89]. The model incorporates four dimensions: (1) the ethical dimension, which places emphasis on the motivations behind actions rather on actions themselves; (2) the security dimension, which examines vulnerabilities brought to life by technologies; (3) the solutions dimension, which examines security countermeasures available for the purpose of information protection; and (4) the moral development dimension, which reflects the personal beliefs of InfoSec professionals with regards to ethical issues in InfoSec.

This model brings to attention the importance of the ethics and morals of IAS specialists. This aspect is overlooked in other models, but is crucial since ethical issues often emerge in IAS (e.g. a financial evaluation of risks to human lives [151] and privacy).

2.8.2.9 A System Model of Security (Jonsson [95, 271])

Jonsson [95, 271] presents a conceptual security model, where the security of a system is considered in terms of input and output. Security, according to [95] encompasses three aspects: confidentiality, integrity and availability. The input characteristic of Jonsson's model - integrity - is designated as protective, whereas the output characteristics - confidentiality and availability - are designated as behavioural characteristics [271]. The main purpose of Jonsson's model [95] is assistance with reasoning about security.

This model is different from other considered models as it represents security as a system with its input and output. However, even this model incorporates security goals and, thus, further confirms their importance.

2.8.2.10 A Security Model for Web Services (Sabbari and Alipour [80])

Sabbari and Alipour [80] suggest a reference model of security in a Service-Oriented Architecture (SOA) environment which has a layered structure. The following layers are included: (1) security principles layer; (2) security policy layer; (3) physical infrastructure layer; (4) SOA governance and risk management and awareness layer; and (5) SOA security precincts layer. This model is technically-oriented and concentrates on InfoSec in an SOA environment, rather than on IAS with its broad scope as it is approached in this thesis. Despite its technical orientation, the model incorporates such non-technical aspects as risk management, governance and awareness.

2.8.2.11 A Conceptual Model of Paths to Information Security Compromise (Ransbotham and Mitra) [82]

Ransbotham and Mitra [82] suggest a conceptual model of the information security compromise process (ISCP) designed from the perspective of a target organisation - an organisation whose security is violated. The ISCP includes (1) the topology of security incidents, (2) the categorisation of countermeasures (access control, vulnerability control, feature control, traffic control, and audit control) and (3) some characteristics of a target organisation. The orientation of the ISCP model on Internet security explains its focus on the technical security countermeasures as may be see from the proposed classification of countermeasures.

The model proposed by Ransbotham and Mitra [82] is the only examined model which is empirically evaluated. It is evaluated using one year alert data from intrusion detection devices. Ransbotham and Mitra [82], in contrast with other papers where the model development process is not covered or superficially mentioned, describe the development process in detail. The model development in [82] relies on many sources such as observations of practice, interviews with experts, the reviews of discussion groups, the reviews of security guidelines and best practices, and on the analysis of the existing models of crime.

2.8.2.12 Information Security Management Framework and Toolbox (Vermeulen and Von Solms [84])

Vermeulen and Von Solms [84] suggest a methodology for effective Information Security Management (ISM). The proposal consist of an ISM framework, methodology and a software tool, the mechanics of which is explained in the proposal. The framework outlines (1) the elements which are essential for the successful management of InfoSec at the preparation stage (top management commitments, organisational aspect, InfoSec standards, and security vision and strategy) and (2) the elements which are required at the implementation and maintenance stage (security requirements, security policy, risk management and follow-up). The ISM methodology outlines the security actions which should be implemented at every stage of the ISDLC. The mechanics of the proposed toolbox are intended to identify security requirements based on business analysis. The matrices that show the correspondence between security requirements, security policy statements and safeguards allow the identification of security policy statements and safeguards and, consequently, procedures that help to achieve specified security requirements. Five security requirements are outlined in the ISM methodology: confidentiality, integrity, availability, authenticity and auditability. In the analysis in Tables 2.6 and 2.7, three parts of this proposal are considered jointly. It is not verified in the paper whether the software tool based on the ISM framework methodology yields valid security policies.

2.8.2.13 A Model for InfoSec Management in Governments (Kumar [85])

In [85], a model for ISM in governments is introduced. In the model, there are seven vertical layers (information security policy, security awareness, identity and access management, network and data security, monitoring, risk assessment, and contingency) in the model which are supported by four horizontal layers (performance measurement (COBIT) and compliance with standards, development, budget and staffing). This model outlines only a set of security countermeasures of various types. Neither a classification of countermeasures is provided nor concepts of the IAS domain other than countermeasures are mentioned in the model.

2.8.2.14 Integral Framework for Information Systems Security Management (Trček [87])

Trček [87] suggests a layered multi-plane model for e-business. Trček [87] states that an organisation should start with the identification of threats to its assets. One plane of the model includes human and human-machine interactions as well as the technical security countermeasures and physical security. Another plane refers to the technological, organisational and legislative aspects of InfoSec. In this model, a central role of people in InfoSec and a need to incorporate security into an IS from the early stages are highlighted. The model acknowledges a legal facet of InfoSec and human-machine interactions as an important aspect to be addressed by InfoSec. To support the model, Trček [87] demonstrates an extended knowledge of every aspect incorporated in the model. However, the model development process and evaluation are not addressed in [87].

2.8.2.15 Information Security Management Best Practice Framework Based on ISO/IEC 17799 (Saint-Germain [88])

Saint-Germain [88] summarises the ISO/IEC 17799 standard into a framework which consists of ten domains: (1) security policy, (2) organisational security, (3) asset classification and control, (4) personnel security, (5) physical and environmental security, (6) communications and operations, (7) access control, (8) systems development and maintenance, (9) business continuity management, and (10) compliance. The framework has a form of a pyramid. At the top of the pyramid is the organisational level whereas at the bottom is the operational one. Although the description of the framework states that the model addresses the managerial, organisational, legal, operational, and technical aspects of InfoSec, none of the domains of the pyramid relates to the legal aspect. This framework is a summary of InfoSec best practices. It outlines only security countermeasures and does not cover other facets of InfoSec. Security goals such as confidentiality, integrity and availability are mentioned in the paper, but are not formally a part of the framework. No links in the papers are drawn between security goals and security countermeasures.

2.8.2.16 The Oracle Information Security Conceptual Architecture (Oracle [81])

In [81], a conceptual model of InfoSec, as it is seen by Oracle, is presented. Oracle attempted to create a reusable reference model of InfoSec which shows the main concepts of the domain. The Oracle model has a layered structure in the center of which is information. The layers of

protection (access control, applications or services, cryptography, policy and process, security & identity management, auditing & monitoring, and business) form secure boundaries within which information is kept. The key elements of the model are distilled from the InfoSec standards such as International Information Systems Security Certification Consortium (ISC2), National Institute of Standards and Technology (NIST), British Standards Institute (BSI)/International Standards Organisation (ISO) 27001:2005, Cloud Security Alliance (CSA) and European Network & Information Security Agency (ENISA). The Oracle model stresses a need of an end-to-end enterprise-wide InfoSec, which assists with the achievement of organisation's goals. The Oracle model is one of a few which incorporates *information* as one of its elements. However, the model considers information to be in a closed environment protected by a circle of technical and organisational countermeasures. This understanding does not comply with the realities of the present environment where information often leaves safe boundaries of an organisation, but still requires protection.

2.8.3 Models Analysis Summary

Tables 2.5, 2.6 and 2.7 summarise the analysis of the discussed models. (The last row of each table shows the RMIAS for the comparison which is drawn at the end of Chapter 3.)

Table 2.5 gives an overview of the models and outlines the basis for the development, evaluation, visual representation as well as the purpose and contribution of each model.

The majority of the analysed models are presented in a format of a position paper. Authors do not present the methodology followed while developing their models and rarely discuss the range of the literature analysed. Table 2.5 shows that only two models ([80, 81]) are accompanied by some analytical evaluation and only one model [82] is empirically evaluated.

The development of a conceptual model or framework must follow scientific principles. The details of a research process (particularly in the qualitative research) allow judgement about plausibility of an outcome of the research [83]. The ability to trace the model development process and to examine information sources analysed may clarify the developer's approach to IAS and to corroborate the plausibility of an IAS model, particularly, in the absence of other evaluation. In some analysed publications [61, 66, 65, 84, 85], a model is built upon the practical experience of the model developer(s) and lacks any further justification or validation. While at the early stage of the IAS domain evolution such an approach was acceptable, the IAS knowledge formalisation domain now calls for the use of more rigorous, explicitly declared methods both for the development of

conceptual models and for their evaluation.

The visual representation and its effectiveness are critical for a conceptual model, since it is, usually, intended for the communication and understanding enhancement purposes. Fifteen out of seventeen analysed models have a visual representation. No formal notation is used and no theory is discussed to support the design of a visual representation in any of the analysed sources. The visual representations of models are guided by pure intuition and the attempt of authors to deliver information in a clear way. The models are often visualised as geometrical shapes (e.g. cube [65, 86, 87] or pyramid [50, 88]). In the majority of models, blocks represent concepts while lines or arrows depict interconnections between concepts.

Table 2.5: The overview of the conceptual models of InfoSec and IA

Author (title), ref., year	Basis for development	Evaluation	Visual Representation	Purpose(s) and Contribution
CIA-traid [94] 1975 - 1987	Summary of the practical knowledge	No evaluation, but wide adoption in practice	Multiple versions	To convey the overarching goals of InfoSec to business and engineering management in a simplified way
McCumber [65] 1991	Practical experience of developer(s)	No evaluation, but wide adoption in practice	Cube (Three dimensions)	To function as an assessment and development framework, to identify and mitigate system vulnerabilities.
Parker [66] 1998	Practical experience of developer(s)	No evaluation	No	An extended set of security goals which replaces the CIA-triad as a model of InfoSec, helps to prevent overlooking of threats
Maconachy et al. [86] 2001	McCumber's Cube updated to incorporated the notion of IA and the concept of defence-in-depth	No evaluation, but accepted as a model of IAS by the fifteen U.S. undergraduate IT programs	Cube (Three Dimensions) and Time	A framework for teachers, students and analysts who are dealing with IA, which promotes a multidimensional view required to implement robust IA programs"

Continued on the next page

Table 2.5 – *Continued from the previous page*

Author (title) [ref.] Year	Basis for development	Evaluation	Visual Representation	Purpose(s) and Contribution
Vermeulen and Von Solms [84] 2002	Practical experience of developer(s) and literature analysis	Software tool supporting the framework is presented, but its correct functioning is not verified	Yes	A framework, methodology and a software tool for InfoSec management
Trček [87] 2003	Experience of establishing health care information system infrastructure	No evaluation	Cube (Three dimensions)	To provide practitioners with steps and background to build optimal and balanced InfoSec solutions
Saint-Germain [88] 2005	ISO/IEC 17799	No evaluation	Pyramid	Summarises a set of best practices and controls required to achieve information confidentiality, availability, and integrity
Lü [93] 2006	Critical analysis of other models	No evaluation	Cube (Three dimensions) and time	To develop an IA plan and baseline strategies, to calculate costs of an IA architecture for large-scale information systems"
Jonsson [95] 2006	Analysis of the existing models of security and integrated models	No evaluation	System input and output	Security of a system presented in the context of its environment and is expressed in terms of input and output, assistance with reasoning about security
BMIS [50, 220] 2008	Adopted from the University of Southern California (USA)	No evaluation	3D pyramid	Promotes a holistic, dynamic, business-oriented approach to InfoSec in the networked environment, exploits system thinking to structure InfoSec

Continued on the next page

Table 2.5 – *Continued from the previous page*

Author (title) [ref.] Year	Basis for development	Evaluation	Visual Representation	Purpose(s) and Contribution
Dark and Harter [89] 2008	Not specified	No evaluation	No	A framework for teaching information security ethics
Al-Hamdani [90] 2009	Synthesis of other models	No evaluation	No	Supports a diligence-based approach to InfoSec based on the use of standards to enforce InfoSec program
Ransbotham and Mitra [82] 2009	Observations of practice, interviews with experts, reviews of discussion groups, reviews of security guidelines and best practices, and analysis of exisitng models of crime	Empirical evaluation using alert data from intrusion detection devices	Yes	Development of empirical constructs and evaluation of their nomological validity, identification of more effective countermeasures
Parker [61] 2010	Practical experience of developer(s) and analysis of security polices of various organisations	No evaluation	Yes	To conduct vulnerability and threat analyses, security architecture revisions, selections and improvements of controls and practices, and their justification and prioritisation for implementation
Sabbari and Alipour [80]2011	Analysis of other models and standards for securing web services	Mapping to standards	Yes	Provides a mapping between areas of SOA and security requirements valid in each area

Continued on the next page

Table 2.5 – *Continued from the previous page*

Author (title) [ref.] Year	Basis for development	Evaluation	Visual Representation	Purpose(s) and Contribution
Kumar [85] 2011	Practical experience of developer(s)	No evaluation	Yes	To assist the IS manager with establishing an InfoSec management programs in governments
Oracle Architecture [81] 2011	InfoSec standards	Analytical validation against criteria derived from InfoSec standards	Yes	Summarises the layers of protection that are required in order to build an end-to-end organisation-wide InfoSec architecture
RMIAS [96] 2013	InfoSec and IA standards, academic and industry publications, security policies, survey of practitioners, informal interview and discussions with practitioners, detailed analysis of the existing IAS conceptual models and frameworks	Analytical evaluation against quality criteria for conceptual models; Empirical evaluation via interviews with IAS experts, case-study and workshops with MSc students	Yes	Synthesis of the existing IAS knowledge in a form accessible to a wide target audience including non-technical and non-security experts

Table 2.6 shows a range of security concepts included in each model. The analysed models use varying terminology and refer to the same security concepts by different names. For consistency, in Table 2.6 the terminology adopted in this thesis is used. For the sake of brevity, not all individual security countermeasures, which are declared in a model, are addressed in Table 2.6. Some countermeasures appear under a summary title. For example, if a model distinguishes such

Table 2.6: Concepts represented in the analysed models of InfoSec and IA

Author (title) [ref.]	Security Goal	Technical Countermeasures	Organisational Countermeasures	Human-oriented Countermeasures	Legal Countermeasures	Other Categorisation of Countermeasures	Information/Information State	Time/SDLC	Threats/Attacks	Vulnerabilities	Cost/Budget/Asset	Physical Infrastructure	System and Environment	Actors/Users	Characteristics of organisation	Information Sensitivity, Form, Location	IAS drivers
The CIA-triad [94]	X																
McCumber [65]	X	X	X	X			X										
Parker [66]	X																
Maconachy et al. [86]	X	X	X	X			X	X									
Vermeulen and Von Solms [84]	X		X			X		X									
Trček [87]		X	X	X	X						Asset						
Saint-Germain [88]		X	X		X	X											
Lü [93]		X	X	X		X		X			Cost						
Jonsson [95]	X	X							X	X			X	X			
BMIS [50, 220]		X	X	X		X											
Dark and Harter [89]		X	X	X	X												
Al-Hamdani [90]	X	X	X	X		X			X								
Ransbotham and Mitra [82]		X	X			X			X	X					X		
Parker [61]	X	X	X	X		X			X								
Sabbari and Alipour [80]	X	X	X	X								X					
Kumar [85]		X	X	X		X		One stage			Budget						
Oracle [81]		X	X				X								X		
RMIAS [96]	X	X	X	X	X		X	X								X	X

countermeasures as access control or/and network security, Table 2.6 shows that technical security countermeasure are addressed by the model. Similarly, if a model incorporates such organisational security countermeasure as top management commitment or security strategy, Table 2.6 depicts that organisational countermeasures are included in the model.

Five analysed models (the CIA-triad and [50, 66, 85, 88] are one-dimensional. They address only one concept (one dimension) of the IAS domain. Three one-dimensional models [50, 85, 88] concentrate on security countermeasures, while the other two on security goals (the CIA-triad and the Parkerian Hexad [66]). The majority of the models [61, 65, 75, 80, 81, 84, 86, 87, 88, 89, 90] are multi-dimensional. In addition to security goals and countermeasures, such important dimensions of IAS as time, cost, information characteristics, threats, vulnerabilities are segregated. A one-dimensional model cannot be seen as a comprehensive overview of the IAS domain, as it only captures one facet of the complex nature of IAS.

Table 2.7: Security goals declared in the analysed models of InfoSec and IA

Author (title) [ref.]	Confidentiality	Integrity	Availability	Accountability	Authentication	Non-repudiation	Authenticity & Trustworthiness	Utility	Possession	Authorisation	Audit/Auditability	Privacy	Federation	Compliance	Interoperability	Manageability	Ease of development
The CIA-triad [94]	X	X	X														
McCumber [65]	X	X	X														
Parker [66]	X	X	X				A	X	X								
Maconachy et al. [86]	X	X	X		X	X											
Vermeulen and Von Solms [84]	X	X	X				A				X						
Trček [87]	P	P	P			P	P										
Saint-Germain [88]	P	P	P														
Lü [93]	P	P	P			P	P										
Jonsson [95]	X	X	X														
BMIS [50, 220]	P	P	P	P													
Dark and Harter [89]																	
Al-Hamdani [90]	X	X	X				A	X	X								
Ransbotham and Mitra [82]																	
Parker [61]	X	X	X				A	X	X								
Sabbari and Alipour [80]	X	X	X	X	X	X				X	X	X	X	X	X	X	X
Kumar [85]																	
Oracle [81]	P	P	P														
RMIAS [96]	X	X	X	X		X	AT				X	X					

Note: X - a goal is a part of a model; P - a goal is discussed in the narration of a model, but is not formally its part; AT - Authenticity & Trustworthiness; and A - Authenticity.

The analysed models do not provide justification for the incorporation of particular dimensions or elements in them. None of the analysed sources discusses the concepts of the IAS which are not included in it or provides any justification for non-inclusion.

Table 2.6 indicates that all analysed models apart from the CIA-triad addresses security countermeasures. In some papers different ways to categorise security countermeasure are suggested (e.g. by time of implementation in [61] or by nature in [65, 86]). In other works, countermeasures are not grouped into any categories. In none of the references a categorisation of security countermeasures at a high level of abstraction, which would encompass all possible types, was found.

The consideration of time in the models (e.g. [86]) is generic, and does not have any practical value. In other models, time is presented as the ISDLC which has more practical value, but in

[85], for example, only one stage of the ISDLC is discussed.

Although cross-organisational information sharing and protection of information outside the organisation's perimeter is mentioned in some works ([50, 65, 86]), it is not explicitly addressed. Other works that concentrate on the Internet and network security (e.g. [82]) are technically-oriented (i.e. consider an IS as a computer and network system) and do not address cross-organisational interactions at levels other than the technical one (e.g. organisational, legal etc.).

Table 2.7 depicts the security goals which are declared in the analysed models. In addition to the omnipresent CIA-triad, authors include in the models such goals as non-repudiation, authentication, possession, authenticity, utility, privacy, compliance, manageability and others. Table 2.7 confirms that in the conceptual models as well as in the IAS literature and system engineering literature as discussed in Section 2.5 there is no an agreed upon set of security goals. Overall, the analysis of the literature with regard to security goals allows to draw two inferences. First, security goals are important in the context of an IAS domain conceptual model. Second, although some attempts are made to produce a comprehensive set of security goals, the sets suggested are not evaluated and their completeness is not verified.

This analysis of security goals in the conceptual models of IAS (Table 2.7 and the analysis of goals addressed in the IAS (Table 2.2) and system engineering literature (Table 5.5 in Chapter 5) highlights the following problems:

- The same goal is referred to by various names in different publications.
- Goals with the same name have different definitions in different sources (various communities input some specific meaning into particular terms).
- Security countermeasures are not distinguished from security goals. The advantage of the notion of *security goal* is that it does not imply the use of a certain measure. A goal outlines the problem to be solved and fosters consideration of all possible alternatives to achieve it [91]. This finally leads to more efficient and cost-effective security solutions. For example, looking at authentication as a goal may lead to the opinion that when a party is authenticated the security problem is solved and, hence, the other facets of the problem stay overlooked. Whereas if a goal is formulated as non-repudiation, then it becomes clear that although authentication is one of the countermeasures which contribute to the achievement of the goal, it does not fully solve the problem because authentication is not always sufficient evidence in litigation [92].

- Lack of clarity to which component of an IS a security goal applies to (e.g. integrity may refer to either data or system integrity, or both. McCumber [65] and Parker [61, 66] consistently refer to the security properties of information. This approach is criticised in [93], since it does not include or make explicit the protection of an IS.

The survey of practitioners, which was conducted as a part of this research project, aimed to identify what security goals IAS practitioners associated with InfoSec and IA. The interviews confirmed that the respondents, in general, were not confident about the goals of either discipline [32]. Thus, among the practitioners as well as in the literature no well-justified comprehensive list of security goals is identified.

2.9 Chapter Summary

This chapter clarified the approach to IAS adopted in this work. IAS is considered as a multi-disciplinary and heterogeneous issue which must be addressed holistically and systematically at the managerial level. This chapter also demonstrated that IAS evolves and that a conceptual model of IAS must be regularly revised.

The summary analysis of the existing conceptual models of IAS was presented in this chapter. Each analysed model has its purpose (Tables 2.5, which undoubtedly along with the perspective and experience of the model developer affects the model (e.g. what elements it embraces). However, there are aspects that unify the models. All analysed models include among their audience a non-technical (primarily, business) audience. The majority of the analysed models attempt to cover the full breadth of the IAS domain [50, 61, 65, 66, 86, 84, 88, 90, 93, 94, 95]. Therefore, it was possible to generalise some conclusions regarding the drawbacks of the models. Moreover, only the examination of the different aspects of IAS and the approaches to it from different perspectives may help to build a "complete picture" of the domain.

The deficiencies ascertained in the existing conceptual models of the IAS domain are summarised below:

- The model development method and the analysed sources of information are not discussed. The transparency of a development method helps to gauge validity and plausibility of a model.

- The classification of security countermeasures, if encountered, does not cover all possible countermeasures. The inclusion of all available countermeasures in the classification enhances the awareness of experts about the heterogeneity and complexity of IAS.

- A model does not provide an alternative for the CIA-triad or a proposed alternative is not justified. The literature analysis testifies (a) the importance of the notation of security goals in the IAS domain and (b) a need for extending the set of security goals beyond the CIA-triad. A new extended set of security goals must be included in a revised conceptual model of IAS to reflect the broadening scope of the domain.

- A model does not address the realities of cross-organisational information sharing. The elements of the analysed models do not explicitly address any characteristics of information related to its location.

- The notion of time within a model has no practical value. The explicit incorporation of the ISDLC in a model promises to have more practical implications than a reference to time in its general sense.

- The visual appearance of a model is not explained or justified. The cognitive effectiveness of a conceptual or reference model is critical since the model is destined for human comprehension. However, authors do not provide any rationale for the design decisions regarding the visual appearance of their models.

- No analytical or empirical evaluation of a model is carried out. The majority of the analysed models are presented in a form of a position paper. The validity of a model typically draws upon the model developer's background and experience. However, in order to evaluate the validity and plausibility of a model more rigorous methods must be applied. According to the recommendations for any qualitative research, ideally, people other than the model developer(s) should be involved in the evaluation of a conceptual model [83]. The need to evaluate the proposed conceptual models of IAS was specifically acknowledged and discussed at the Security Ontology workshop at the ARES 2013 conference, where the RMIAS along with its evaluation was presented.

The analysis shows that none of the existing models adequately represents the IAS domain in its current reincarnation. This calls for a new revised conceptual model of IAS and an updated list of security goal as a part of the model. The next chapter introduces the Reference Model of Information Assurance & Security (RMIAS) which attempts to address some of the drawbacks

enumerated above. In section 4.5, the above listed bullet points are revisited and it is deliberated how the RMIAS addresses them.

Chapter 3

The RMIAS

This chapter introduces the Reference Model of Information Assurance & Security (RMIAS). The RMIAS draws upon the IAS literature and existing models of IAS, as discussed in the previous chapter. The RMIAS endeavours to overcome the limitations of the existing conceptual models of IAS and to address the recent trends in the IAS evolution. In 2013, the RMIAS was presented at the Eighth International Conference on Availability, Reliability and Security (ARES) [96]. Before exposing the reader to the RMIAS, this chapter reports on the RMIAS development methodology and justifies the choice of a reference model as the form of knowledge representation in this thesis.

3.1 Development Methodology

The RMIAS evolved as a result of the investigation of the following sources: (1) InfoSec and IA standards and best practices such as the ISO/IEC 27000 family of standards, the National Information Assurance Glossary, published by the United States Committee on National Security Systems and Control Objectives for Information and related Technology (COBIT) framework (Chapter 2); (2) the security policies of the organisation the author of the thesis collaborated with during this research project (Section 4.4.1); (3) the existing models and frameworks of IAS (Chapter 2); (4) informal interviews with experts and discussions in IAS professional groups on LinkedIn; (5) the materials of the education programs for InfoSec and IA modules at the School of Computer Science & Informatics, Cardiff University.

First, the IAS literature (standards, industry and academic publications) were examined in order to establish the scope of the IAS domain. As the result of this analysis, the definitions of InfoSec and IA, which are adopted in this thesis, were produced. The analysis also helped to identify the security goals which are associated with the IAS domain. While analysing the IAS domain,

recent trends in the domain were also examined. This literature analysis is presented in [7] and is reproduced in this thesis in Sections 2.1 - 2.4.

The literature analysis resulted in establishing the scope of the IAS domain and its goals, and adopting an holistic approach to IAS. Consequently, it influenced the range of models/frameworks included in the review which was performed prior to the development of the RMIAS. Section 2.8 contains the systematic review of the existing models/frameworks of IAS.

As the result of the literature analysis, the main concepts of the IAS domain were pinpointed and included in the provisional version of the RMIAS as dimensions. Next, research on every dimension was conducted in order to develop the structure of the dimension in depth (i.e. the security development life cycle model, the information taxonomy, the set of security goals and the classification of security countermeasures). Finally, the interrelationships between the dimensions (which are illustrated with arrows in Figure 3.1) were identified and formulated along with the drivers behind IAS decisions (which are shown under the arrows in Figure 3.1).

While attempting to organise and structure IAS knowledge, research was carried out into the various forms of knowledge representation. A reference model was chosen as the form of representation to be exploited in this research project. Section 3.2 and Appendix A.3 contain the details.

The RMIAS is the culmination of the analysis of the IAS literature and is a synthesis of the existing knowledge of the IAS domain. The Best Evidence Synthesis (BES) approach [97] was exploited while developing the RMIAS. This method was chosen because it provides guidance on synthesising knowledge and helps to retain focus while choosing knowledge to be included in a synthesis. While the BES approach provides instructions on the inclusion of studies in an analysis, in this thesis the BES approach was applied to the inclusion of concepts in the RMIAS. The BES approach recommends relying on the quantitative characteristics of studies (when such characteristics are available) for their inclusion in a review. However, the sources examined in this research usually do not provide any quantitative data. In this instance, the BES approach recommends identifying *a priori* criteria for the inclusion/exclusion of knowledge into a synthesis.

In this thesis, the following non-quantitative criteria were checked for the inclusion/exclusion of concepts into the RMIAS (in the brackets the justification for each criterion is given):

1. A concept *should be widely known in the IAS domain* and must be discussed in several academic and industry sources (in order to be included in a reference model a concept shall be

significant within the domain and acknowledged as such in other publications (germaneness to the issue at hand [97]));

2. A concept *should be easy to grasp and should not require profound technical or security knowledge* (this criterion is based on the specifics of the RMIAS target audience which includes a broad range of experts with various backgrounds, not necessarily technically- or security-oriented[1]);

3. A concept *should be important and make sense from the business perspective* (IAS does not exist for its own sake. For an organisation IAS is only one of many means of achieving business goals. The target audience of the RMIAS includes business experts. The RMIAS shall express IAS concerns in a language and at a level that is understandable by business experts, who take strategic decisions about investing in IAS programs); and

4. A concept *should be generic and valid within the majority of organisations*, a concept should not be technology- or organisation-specific (the RMIAS is an abstraction which with some adaptation shall be applicable in a large number of organisations).

Thus, the choice of these criteria is explained by the purpose and target audience of the RMIAS.

It was demonstrated in the previous chapter that security goals play an important role in IAS. Therefore, the RMIAS incorporates security goals as one of its dimensions. However, the existing literature does not provide a commonly agreed list of security goals. In this research project, a generic, broadly applicable set of eight security goals was identified and included in the RMIAS.

In order to develop the set of security goals the following route was pursued:

1. An integrated list of goals was produced to include all goals referenced in the analysed literature (see Tables 2.2 and 2.6);

2. Each identified goal was examined individually;

3. The goals with similar or strongly overlapping meaning were either excluded or merged (e.g. the notion of utility is included in the notion of availability as discussed in Section A.6.0.0.2, possession is addressed by the Location attribute of the RMIAS as demonstrated in Section 3.5.3);

[1]Further in the thesis, when a reference is made to the target audience of the RMIAS and Secure*BPMN, it refers to a multi-disciplinary group of experts which includes a broad range of experts with various backgrounds, not necessarily technically- or security-oriented.

4. Security countermeasures were excluded from the list (e.g. access control, authorisation, audit, awareness and the like were excluded as they outline "how", rather than "what" should be achieved);

5. A security goal was included in the final set if it met the following criteria:

   - A goal has a unique name;
   - A goal has a unique meaning which is not addressed by any other goal(s)[2];
   - A goal is meaningful both in the IS design and business contexts; and
   - A goal is discussed in more than one analysed source.

6. The definitions of the goals in the final set, along with the applicability of the goals to different components of an IS, were discussed with an IAS expert, who has over 25 years of experience in the IAS domain both in academia and industry. During the 1.5 hour workshop, where the discussion took place, each security goal and its applicability rules were debated until the agreement was reached.

For a qualitative research to be rigorous and plausible, (a) the research process must involve people others than a researcher and (b) the outcome of research must be verified and evaluated with the involvement of people others than a researcher [83]. During the RMIAS development process, the evolving versions of the model were iteratively discussed with a number of IAS practitioners, academics and PhD students specialising in various aspects of IAS. The RMIAS was adjusted based on the received comments in order to improve its clarity, precision and accuracy. After the development was completed, the RMIAS was evaluated via interviews with IAS experts and workshops with MSc students. Chapter 4 is devoted to the evaluation of the RMIAS .

[2]The pivotal purpose of a security goal is to help with the identification of security countermeasures mitigating threats of a certain category. Since the same security countermeasure may help to achieve different goals (e.g. biometrics and digital signature contribute to confidentiality, integrity, accountability and non-repudiation; a sealed envelope guarantees both confidentiality and integrity), an overlap of security goals is unavoidable. Using this logic, confidentiality strongly overlaps with privacy because one of countermeasures which helps to achieve both goals is access control. Nevertheless, the notion of privacy has some essential aspects that are not covered by confidentiality (e.g. legal obligations to protect private information or a need to involve information owners in defining a level of exposure of their private information). Therefore, as long as a goal has a unique component it was included in the final set of security goals.

3.2 Conceptual and Reference Models

Any knowledge area has either an explicit or assumed conceptual model, which describes the phenomenon being investigated, "*maps reality, guides research and systematizes knowledge*" [33]. A conceptual model should outline (1) inherent elements of a system; (2) the relationships between the elements of a system; (3) changes in the elements and their interrelation; and, ideally, (4) research directions [33]. A conceptual model is usually graphically represented [98]. The pivotal purpose of a conceptual model is to facilitate understanding and communication among interested parties of a modelled system or domain [99, p.244].

Conceptual models, which strive to represent a problem at the industry level and to capture domain knowledge, are known as reference models [99]. OASIS [100] provides the following definition of a reference model:

Definition 5. *A **Reference Model** is an abstract framework for understanding significant relationships among the entities of some environment. It enables the development of specific reference or concrete architectures using consistent standards or specifications supporting that environment. A reference model consists of a minimal set of unifying concepts, axioms and relationships within a particular problem domain, and is independent of specific standards, technologies, implementations, or other concrete details.*

The Zachman Framework [101], the OASIS Reference Model for Service Oriented Architecture [100], the Reference Model of Open Distributed Processing (RM-ODP), published as an ISO/IEC standard [102], are concrete examples of reference models.

There are three main characteristics of a reference model [98]:

1. Best practice: It summarises the best practices of a modelled domain.
2. Universal applicability: It represents an entire domain. It is generic and satisfies the requirements of multiple organisations [103]. A reference model is adequate (with some minor adjustments) for any organisation within the domain.
3. Reusability: It serves as a template of an IS which provides information and communication services for organisations within the domain.

In knowledge representation, five levels of knowledge representation are distinguished: linguistic, conceptual, epistemological, logical and implementational. The brief introduction to knowledge

representation is contained in Appendix A.3, where five levels of knowledge representation are described and various forms of IAS knowledge representation are examined.

A reference model represents knowledge at the conceptual level and is intended to convey the knowledge in a human intelligible way. Since the motivation of this research is to present the IAS knowledge in a form which is accessible to a wide audience and which helps to facilitate effective human education and communication, a reference model is the form of knowledge representation that best suits the spirit of this research.

The advantage of a reference model and the rationale behind the choice of this form of knowledge representation in this thesis is that a reference model is notation-free and representation-neutral. One of the first restrictions towards the precise knowledge representation is a form of representation used, i.e. a specific modelling notation or language which defines "*how and what to see in the world*" [104]. A representation defines what is important and what should be ignored, what can and cannot be expressed about the object. By choosing a particular representation, a user adopts a specific viewpoint which, by definition, is restrictive since each form of representation brings into focus some aspects and overlooks others. The chosen representation strongly affects the perception of a represented object [104].

A reference model is not confined in this sense since there are no formal rules on what can or cannot be represented. This makes a reference model more flexible. The absence of the need to know/learn representation rules broadens the audience for whom a reference model is accessible. The existing models of IAS, which are reviewed in Section 2.8.2, confirm that when it comes to the representation of a complex and heterogeneous phenomenon, a reference model as a notation-free form of knowledge representation is often preferred. In view of the above, the IAS knowledge in this thesis is represented in the form of a reference model (Section 3.3).

3.3 Overview of the RMIAS

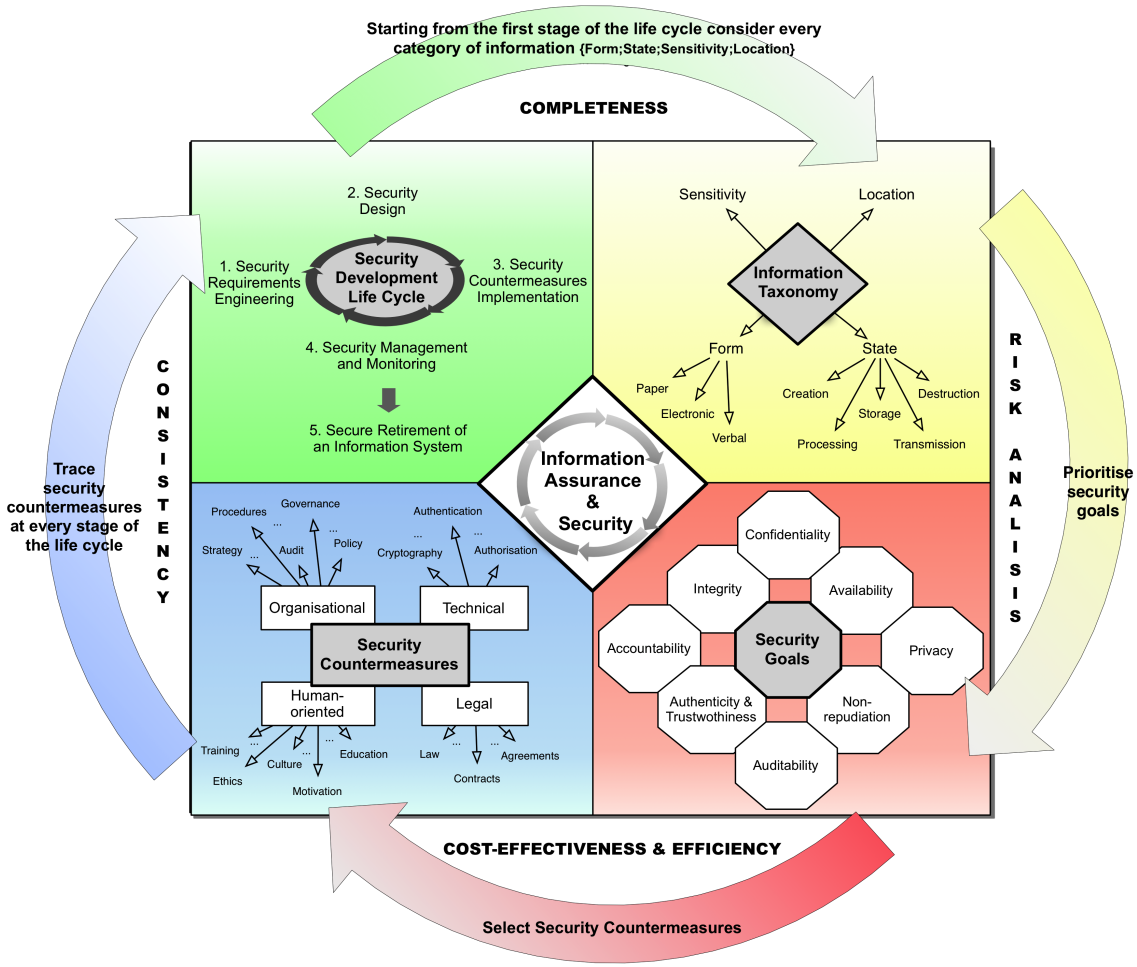


Figure 3.1: The Reference Model of Information Assurance & Security (RMIAS)[3]

[3]The security countermeasures dimension outlines only some countermeasures related to each type, but not the exhaustive lists. Within the information taxonomy dimension, attributes *location* and *sensitivity* possess values specific to an organisation (Sections 3.5.2 and 3.5.3).

The RMIAS, which is depicted in Figure 3.1, has four dimensions:

- **Security Development Life Cycle Dimension** (top left quadrant) illustrates the progression of IAS along the Information System Development Life Cycle (ISDLC);
- **Information Taxonomy Dimension** (top right quadrant) outlines the characteristics of information being protected;
- **Security Goals Dimension** (bottom right quadrant) outlines the set of eight security goals, also referred to as the IAS-octave.
- **Security Countermeasures Dimension** (bottom left quadrant) categorises security countermeasures.

The four concepts, which the dimensions of the RMIAS represent (i.e. security life cycle, information and its characteristics, security goal and security countermeasure) were included in the RMIAS because they satisfy the inclusion criteria outlined in Section 3.1. The dimensions originate and are adopted from the examined existing models of IAS. The RMIAS summarises the models examined in the previous chapter and extends the models proposed by McCumber [65] and Maconachy et al. [86]. The origin of each dimension and how it is extended in the RMIAS explained in the following sections presenting each dimension.

The literature analysis confirms that there is research and industry publications related to each concept included in the RMIAS. These publications are discussed in the subsequent sections of this chapter where the importance of each included concept within the IAS domain is discussed.

While presenting the key concepts of IAS, four dimensions of the RMIAS do not overlap and do not duplicate each other. The RMIAS, starting from the top right quadrant, outlines (1) what information an organisation has and needs to protect (the information taxonomy dimension), (2) what must be achieved in terms of security for each piece of information (the security goals dimension), (3) how the identified goals may be achieved (the security countermeasures dimension) and (4) the cycle of security activities ensuring that the concepts of other three dimensions are adequately addressed at every stage of the life cycle (the security development life cycle dimension).

Table 2.6 contrasts the dimensions of the RMIAS with the dimensions of other models, which are examined in the preceding chapter. This table confirms that apart from the RMIAS only the Maconachy et al. model [86] incorporates the same four dimensions as the RMIAS. Other models

overlook some key security concepts. For example, only four models [86, 84, 93, 85] address time or the ISDLC. However, these four models do not specifically concentrate on the security development life cycle and its stages [86], or address only one stage of the life cycle [85], and do not include such concepts as information and its characteristics [84], security goal and information [93, 85]. The differences between the Maconachy et al. model [86], with which the RMIAS has the most similarity in terms of the outlined dimensions, are in the inner structure of the dimensions: (1) the RMIAS outlines a wider list of security goals within the security goals dimension (Table 2.7), (2) the RMIAS distinguishes legal security countermeasures which are not addressed in [86], (3) the RMIAS outlines more detailed information taxonomy than in [86] and (4) Maconachy et al. [86] although discuss time, but depict it only as a time line, without distinguishing separate stages of the security development life cycle as opposed to the RMIAS. More detailed comparison of the RMIAS with other models is drawn in Chapter 4, after the RMIAS is thoroughly described in this chapter.

Based on the literature analysis, it is hypothesised at this point that four dimensions distinguished in the RMIAS are compulsory and sufficient for the understanding of the IAS domain by the target audience of the RMIAS (i.e. a multi-disciplinary team of experts) at the chosen high level of abstraction. This assumption is empirically tested in Chapter 4 where the completeness of the RMIAS is evaluated via interviews with IAS expert, workshops with MSc students and a case study.

The RMIAS is a generic abstraction. Before its use in the context of a specific organisation the following elements of the RMIAS should be adapted:

1. The generic security development life cycle should be replaced with the one specific to the organisation (Section 3.4); and

2. The information taxonomy should be extended with the information sensitivity classifications and the location classification which are specific to the organisation (Sections 3.5.2 and 3.5.3).

Sections 3.4-3.7 provide the description of each dimension of the RMIAS, and outline the importance of the dimension in the IAS domain and the justification for its inclusion in the model. The interrelationships between the dimensions, which are illustrated with arrows in Figure 3.1, are explained in Section 3.8. Section 3.10 gives an account of the RMIAS visual appearance.

3.4 Security Development Life Cycle (Time) Dimension

In agreement with Mochonachy et. al. [86], who introduced time as the fourth dimension of IAS, this thesis acknowledges the importance of time in IAS. However, one clarification is required.

Time in IAS could be seen from two perspectives. The first perspective is the general notion of time, where time is considered as a continuum in which IAS, as the discipline and area of practice, evolves in response to the fluctuation of the environment. Any model of IAS presents a snapshot of the domain at a particular period of time and reflects its contemporary environment, i.e. (1) the IAS knowledge, acquired by a certain point in time, (2) a variety of existing security countermeasures, (3) a level of connectivity and information sharing along with the threats they evoke and (4) social security and privacy expectations and awareness, (5) IAS standards and best practices in force. No conceptual model, including the RMIAS, could be valid forever. Any major change in the environment, which affects security, calls for the revision of a conceptual model of IAS. Thus, reflecting the changes in the domain, its growing scope and the increasing number of goals, conceptual models of IAS also evolve.

The understanding of time, in its general notion, is important for an IAS specialist, since (1) it provides the tool for studying and understating the history of IAS, and (2) it prevents the tendency to anchor a model of the domain and highlights a need for its regular revision. However, time in this general sense as described above has little practical application in the context of the deign of a secure Information System (IS).

The second perspective of time in IAS is representing it as the security development life cycle within a particular IS. This perspective of time is more pragmatic and better compliant with the context of the IS design. This second perspective is not opposite to the first perspective, but rather represents one of the subsets within the general notion of time.

The rationale for the incorporation of the security development life cycle into the RMIAS is two-fold. First, it highlights a need to address IAS consistently throughout all stages of the ISDLC. *"Security is most useful and cost-effective when such integration begins with a system development or integration project initiation, and is continued throughout the SDLC*[4] *through system disposal"* [105, p.19]. Second, it enables the establishment of a stage-dependent sequence of IAS activities (security procedures).

[4]SDLC - system development life cycle.

Many standards (ISO/IEC 27000 series; the Federal Information Security Management Act (FISMA); Office of Management and Budget Circular A-130, Appendix III; NIST Special Publication 800-64) require security to be addressed starting from the early stages of the ISDLC. In practice, IAS is often treated as an afterthought and left until implementation or maintenance stages [24].

The security development life cycle consists of several stages with each having its purpose and outcome [106]. Official publications propose different ISDLC models and different security development life cycle models, which are overviewed in detail in Appendix A.4. In fact, standards (e.g. [106, 105]) do not require an organisation to follow any particular ISDLC, but require it to choose or tailor, and consistently follow one life cycle model that better suits the organisation. The security development life cycle should be adapted to the ISDLC chosen by an organisation, because IAS, does not exists for its own sake, is an integral part of an IS and could not be considered separately from it. The security development life cycle reflects the progress of IAS along the ISDLC[5].

The RMIAS incorporates a generic security development life cycle, which sums up the security development life cycle models considered in Appendix A.4, and has five stages as depicted Figure 3.2. Appendix A.4 also shows the mapping between the stages of the security development life cycle distinguished in the RMIAS and the stages encountered in other publications. The detailed description of security activities and expected outcomes within each stage of the life cycle is contained in [105].

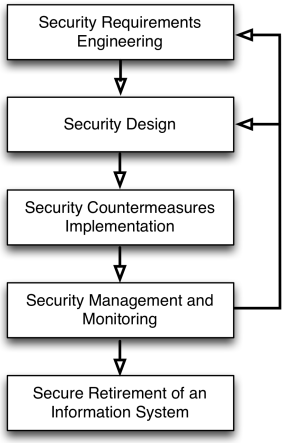


Figure 3.2: A Generic Security Development Life Cycle

[5]It is important not to confuse a software development life cycle with the ISDLC. As stated in Definition 4 software is only one of the components of an IS.

The remainder of this section concentrates only on the first two stages of the life cycle, namely security requirements engineering and security design, because this thesis tackles the problem of addressing IAS at these two stages. The place and role of the RMIAS and Secure*BPMN in the security development life cycle is outlined below.

During the security requirements engineering stage (initiation) a risk analysis is performed and high-level information security policy requirements are defined [105, Sec. 3.1]. The typical deliverable of this stage would be an ISPD, which may be enriched with additional details during the design stage. The RMIAS plays a critical role at this stage. It helps to (1) inventory information assets an organisation has (the information taxonomy dimension (Section 3.5)); (2) ensures that all potential threat situations are examined (the security goals dimension (Section 3.6)); and (3) helps with the identification of security countermeasures mitigating possible threats (the security countermeasure dimension (Section 3.7)). The process of developing a security policy document using the RMIAS is described in Sections 3.8-3.9 and tested in a case study and workshops as described in Chapter 4.

During the second stage, an organisation designs the system, producing a set of system models. For this purpose, it "*should simultaneously define the system's security and functional requirements*" [105, Sec. 3.2]. This is where Secure*BPMN comes into play and assists with doing exactly that. As already, discussed in the introduction (Section 1.1.4), the representation of security aspects within business process models enables the involvement of business (and other non-technical experts), technical and security experts into the design of a secure IS, and facilitates the concurrent consideration of functional and security requirements. According to [105], non-functional security requirements are not limited to technical countermeasures (e.g. encryption, access control and log etc.), but must also address organisational (e.g. background check for a system developer) and human-oriented (e.g. awareness and training) countermeasures. Secure*BPMN, which builds upon the RMIAS, allows the consideration of the three above named types of security countermeasures and goes even further by brining in the radar of attention legal countermeasures as well (Chapter 6).

3.5 Information Taxonomy Dimension

McCumber [65] claims that in order to identify appropriate security goals and, subsequently, appropriate security countermeasures for a specific piece of information, it is sufficient to know the

state of information. McCumber [65] distinguishes three possible states of information: transmission, storage and processing.

The RMIAS argues that knowing the current state of information is insufficient for identifying the security countermeasures the information requires. The RMIAS incorporates the Information Taxonomy which helps to understand fully the nature of information being protected. In addition to taking into account the state of information as suggested in [65], the RMIAS also considers Form, Location and Sensitivity. Further, the RMIAS extends the three states of information described by McCumber [43] with additional two states, namely creation and destruction. As the result, the RMIAS provides for a better grounded choice of security countermeasures.

In the RMIAS, information[6] at any moment in time is characterised by the following attributes:

1. Form (Format),
2. Sensitivity,
3. Location, and
4. State.

These four attributes are described in the subsequent subsections.

The sensitivity of information may change over time and should be revised regularly. The state, form and location of information change numerous times during the information life cycle, while information sensitivity changes less frequently.

The combination of these four attributes characterises information and assists with the identification of relevant security goals and countermeasures.

3.5.1 Information Form

Information may be in one of three forms (formats):

1. Paper,
2. Electronic, or

[6]Further in the text, the term *information* refers either to a document, a piece of information in a particular document, a database, a record in a database or verbal message.

3. Verbal.

This forms are convertible. The same information may be in any of these three forms. The bank account security number, for example, may be sent in a paper form by post, it may be sent electronically by email or passed verbally by phone. The security countermeasures required depend on the form of information. A letter must be sent by recorded delivery, an email must be encrypted, while during a telephone conversation the identity of a client must be verified.

Sensitive information may be communicated/transmitted not only in the paper or electronic form, but also verbally. Verbally transmitted information requires different security countermeasures such as, for example, (1) an employee confidentiality or non-disclosure agreement, (2) a candidate background check for the position which involves dealing with sensitive information, etc. The RMIAS explicitly distinguishes verbally transmitted information. None of the models considered in Section 2.8.2 distinguishes verbally transmitted information as the form of information which requires protection. Being more precise, none other model considers the form of information at all (Table 2.6).

3.5.2 Information Sensitivity

"Not all information needs to be protected at the same level,
but all information needs to be protected."
McKnight W. L. [107, p.6].

There are numerous classification schemes. The multilevel security information classification scheme (used by NATO governments during the Cold War) encompasses the following categories: Top secret, Secret, Confidential and Unclassified [49, p.276]. The Jericho Forum proposes the following classification scheme: Highly Sensitive, Sensitive, Normal Business and Public [108]. The UK government classification scheme was as follows: Top Secret, Secret, Confidential, Restricted, Protect, and Unclassified [109]. In 2013, the UK government classification scheme was revised and from April 2014 is replaced with a new scheme: Official, Secret and Top secret [110]. The information sensitivity classification and colour-enhanced labelling scheme known as the Traffic Light Protocol [108, 111] proposes the following classification: Public, Normal Business, Sensitive, and Highly Sensitive. The Traffic Light Protocol was put forward to support safe sharing of sensitive information and adopted by National Infrastructure Security Co-ordination Centre

(NISCC), UK [111]. The Traffic Light Protocol is also in use by many official and private organisations worldwide [112, 113].

By incorporating the *Sensitivity* attribute in the information taxonomy, the RMIAS points out at the need to classify information by sensitivity and to take it into account while developing security policies and procedures. However, the RMIAS does not impose any specific classification scheme because the scheme depends on the specifics of an organisation, i.e. size, domain, the nature of activities, etc. ISO/IEC 27002:2005 [69] requires an organisation to classify information by sensitivity, criticality and value to the organisation, and label it appropriately. An organisation shall develop an information classification scheme according to its business needs. Following ISO/IEC 27002:2005 [69], the RMIAS prompts an organisation to develop and use the document classification scheme that better suits the organisation's specifics, rather than dictates to adopt some specific scheme. When the RMIAS is exploited by a specific organisation, the information taxonomy must be extended with the sensitivity classification which is used by the organisation. The example is provided in Section 3.9.

In this thesis, a case study of Translate, a Small and Medium-size Enterprise (SME) which provides translation services, is exploited. The description of Translate is outlined in Appendix A.5. In this thesis, the document classification scheme of Translate is adopted as a sample classification scheme. Translate classifies its information as follows: *Public*, *Proprietary*, *Restricted Sharing* and *Confidential*[7]. The details of the classification scheme could be found in Table 3 in Appendix A.5. The scheme is based on the Traffic Light Protocol, but the names of the sensitivity levels are adapted to better reflect the nature of the information of Translate. This classification scheme is concise and generic to suit the needs of many SMEs and, therefore, is well fit as an example. However, the use of the classification scheme of Translate as an example in this thesis by no means implies that this scheme is superior to others or is recommended for general use.

There are two reasons behind the inclusion of information sensitivity into the Information Taxonomy dimension of the RMIAS.

First, security goals and countermeasures are defined on the basis of information sensitivity [69, Sec. 7.2]. Using Translate's classification scheme, for a document classified as *Restricted Sharing*, confidentiality has high priority, whereas for a document which is classified as *Public* (e.g. press-release), confidentiality is not essential while integrity is. Accordingly, different security

[7]Further in the text, the sensitivity levels of documents are capitalised and italizised to enhance readability.

countermeasures should be applied to the information of the different levels of sensitivity. For example, while a *Public* document may be sent by ordinary post, a document which is classified as *Confidential* should only be sent by special delivery.

Second, classifying information by sensitivity is one of the mechanisms for enhancing information protection while information is shared cross-organisationally [108]. Within an information sharing community members often operate their own bespoke classification schemes. In order to protect cross-organisationally shared information, the information classification and labelling schemes of organisations involved in information sharing should be in agreement. ISO/IEC 27010:2012, Sec. 7.2 [268] states that "*care should be taken in interpreting classification markings assigned by other members of an information sharing community*". The consensus regarding the classification scheme which is in use by an information sharing community is crucial, but hard to achieve because, first, information has various values for different organisations and, second, even similar classification and labelling schemes do not automatically imply a similar level of protection being applied. The incorporation of sensitivity into the information taxonomy of the RMIAS points out to the need for consistent handling and protection of information in an information sharing community, and for the harmonisation of classification and labelling schemes.

3.5.3 Information Location

Risk to information and, consequently, the required security countermeasures, apart from the form and sensitivity of information, also depend on the location of information [108]. Sensitive information processed on a laptop at an internet café should be protected differently from the same information processed on a desktop in an organisation's office. The location of information acquires particular importance in information sharing communities. Within each location, it is important how much control the owner of information has over the environment and information itself.

Parker [66] proposes to consider possession/control as a security goal and included it into his model of InfoSec. Possession is defined by Parker as "*[t]he holding, control, and ability to use information*". Possession refers to physical contact with data and also to copying or unauthorised use of intellectual property (such as films, music, software). Parker claims that loss of possession does not necessarily lead to a breach of confidentiality (e.g. if a stolen CD is not decrypted by a thief).

The RMIAS does not include possession/control as a security goal, but incorporates the location

attribute of information to address a similar concept. The possession or location of information is not seen in this thesis as a security goal, but rather as one of the characteristics of information which affects the choice of security countermeasures.

Another aspect the location attribute brings to light is that location or physical possession does not assume information ownership. A software developer may not take away the code he works on and which is stored on his\her laptop when leaving a company. Although a software developer possesses the program code on his\her laptop, the ownership belongs to the employer [66]. Outsourcing is another example. A service provider (e.g. cloud provider) physically possesses information, but ownership is retained by a customer. Clear answers to such questions as to *who owns information* and *where it is physically located* help to identify adequate security countermeasures. In the example with a cloud provider, a customer may prefer to make information unavailable to the service provider personnel by storing it in an encrypted form.

The categorisation of locations is organisation-specific. An organisation, who exploits the RMIAS, categorises locations to the granularity which suits its needs. A category of locations includes the locations in which similar security countermeasures may be applied. The grouping of locations simplifies the formulation of security policies. Instead of producing multiple security policy statements for every location, a generalised statement for a group of locations may be produced.

In this thesis, the following categorisation of locations is suggested and is exploited in the case study of Translate:

- *Controlled* - locations where information is under the full control of the organisation (e.g. organisation's offices);
- *Partially controlled* - locations where information is physically possessed by other organisations with which the organisation has contractual relationships (e.g. IT-service provider, third parties storing or processing information on behalf of the organisation, business partners and employees' homes); and
- *Uncontrolled* - locations other than those falling into the previous two categories (e.g. meeting rooms in hotels, airports and other public buildings).

This categorisation proved to be sufficient in the context of an SME in the case study of Translate. However, it is explicitly acknowledged that more elaborated categorisations of locations may be required with other organisations. The RMIAS, as in the case of information sensitivity, does

not dictate the specific categorisation of locations which must be exploited by an organisation. However, the RMIAS highlights the need to consider the location of information when identifying security goals and countermeasures.

3.5.4 Information State

The state of information, along with its form, sensitivity and location, defines security countermeasures to be implemented to protect the information. During its life cycle, at every specific moment, information may be in one of five states: creation, transmission, storage, processing or destruction (Figure 3.3). Information may change its state between transmission, processing and storage numerous times. Information reaches the states of creation and destruction only once at the beginning and at the end of its life cycle respectively.

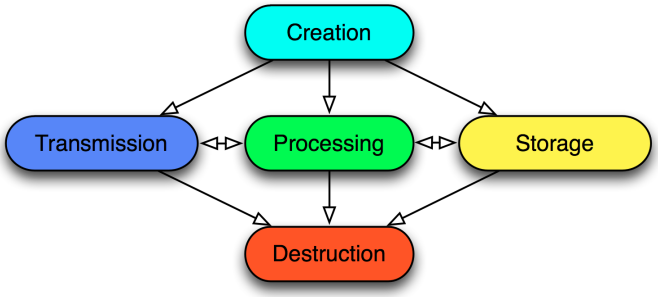


Figure 3.3: Information Life Cycle illustrates possible states of information

Not considering the creation and destruction states of information (which is observed in [65, 86]) is erroneous. The analysis of information security policies of various organisations confirms that the protection of information at the states of creation and destruction (as well as at the other three states) is important and is thoroughly addressed in security policy documents. ISO/IEC 27001 [114, A.10.7.2] also covers safe destruction of information. Therefore, creation and destruction are captured in the RMIAS.

During creation, the completeness and correctness of information must be ensured (integrity), the appropriate provenance data must be set (auditability and accountability), the appropriate level of sensitivity must be assigned and the corresponding marking/labelling applied (confidentiality and privacy). The destruction of information should be controlled, audited and executed in a lawful way (e.g. the Data Protection and Sarbanes-Oxley Acts [115] require confidential financial and personal information to be deleted with special care). Thus, the confidentiality of information must

be ensured even at the state of information destruction and appropriate security countermeasures should be selected to meet regulatory requirements.

The protection of information during transmission, processing and storage is addressed in detail in [65].

3.5.5 Information Categories Examples

The set of four attributes described above (form, sensitivity, location and state) defines an information category - a group of information assets that have similar characteristics. An information category is a basis for the specification and selection of security goals and countermeasures. This section outlines some examples of information categories based on the case study of Translate and discusses security countermeasures that may be required for these categories of information.

Thus, at each moment, information is characterised by a combination of attributes *Form*, *State*, *Sensitivity*, and *Location*:

$$\mathrm{I} = \{\mathrm{F}, \mathrm{S}, S_n, \mathrm{L}\},$$

where

- I - category of information;
- F - form and F ∈ {paper, electronic, verbal};
- S - state and S ∈ {creation, transmission, storage, processing, destruction};
- S_n - sensitivity and Sn ∈ {*Public*, *Proprietary*, *Restricted sharing*, *Confidential*};
- L - location and L ∈ {controlled, partially controlled, uncontrolled}.

For example, Translate - an SME introduced in Section 3.5.2 - produces a monthly financial report for internal use only. The attributes of the report are as follows: form - *electronic*; state - *creation*; location - *controlled*; sensitivity - *Confidential*. At this stage the document should be labelled accordingly with the classification scheme and saved in the directory to which only designated people have access.

If Translate sends a paper document classified as *Restricted sharing* to another organisation, with which Translate have contractual relations, and the organisation places the document in a folder

for later consideration, the document has the following attributes: form - *paper*, state - *storage*; location - *partially controlled*; sensitivity - *Restricted sharing*. For this category of information, Translate must ensure (1) that the document is marked appropriately, when it is sent to the external organisation, and (2) that the organisation the document is sent to is bound by the agreement to deal with the information in accordance with Translate's classification and policies.

There may be a situation where a document classified as *Confidential* escapes the perimeter of Translate (e.g. an employee by mistake sends a *Confidential* document to an external party). The attributes of the document are as follows: form - *electronic*; state - *processed*; location - *uncontrolled*; sensitivity - *Confidential*. This set of attributes flags a dangerous situation and prompts the planning of security countermeasures required to prevent information falling into this category (e.g. email content control system prevents documents classified as *Confidential* to be sent to external email addresses).

3.6 Security Goals Dimension

*A **Security Goal** is a desirable ability of an IS to resist a specific category of threats*. The RMIAS incorporates as one of its dimensions the IAS-octave, a set of eight broadly applicable security goals which includes Confidentiality, Integrity, Availability, Accountability, Authenticity/Trustworthiness, Auditability, Non-repudiation and Privacy (Figure 3.4). This set of goals was identified following the methodology which is outlined in Section 3.1.

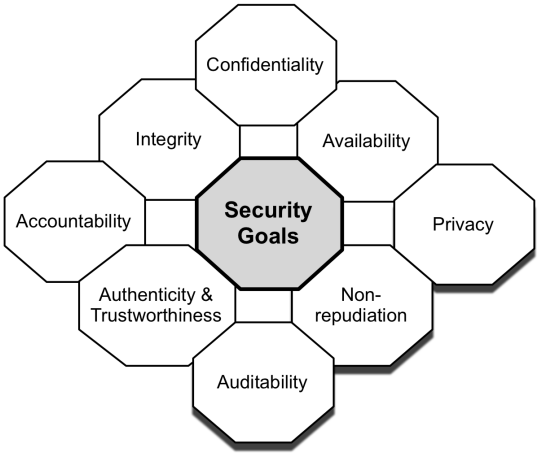


Figure 3.4: The IAS octave

Table 3.1 states the definitions of the security goals in the IAS-octave. The detailed discussion of each security goal included in the IAS-octave is contained in Appendix A.6. Table 3.1 also lists sources which were analysed in order to understand each security goal.

In Table 3.1, the term "system" should not be interpreted as a "technical system", but in a broad sense according to the definition of an IS adopted in this thesis (Definition 4). It was found that replacing the term "system" with the term "organisation" in the context of Table 3.1 provides clarity for a non-technical audience.

The IAS-octave extends the CIA-triad. Based on the literature review and the exploited development methodology (Section 3.1), it is hypothesised at this stage that the IAS-octave is a complete, for now, set of security goals, i.e. the IAS-octave covers all security threats that are currently known. The completeness of the IAS-octave is further ensured via interviews with 26 IAS experts as discussed in the following chapter. The IAS-octave, as with any other set of security goals, requires regular revision over time in order to include newly emerging threats.

Each security goal is not equally important for every organisation or every information. For example, if an organisation deals with no private data, then privacy for this organisation is less significant than for the organisation which processes large amount of private information. Every organisation must prioritise security goals according to its specifics, based on the outcomes of risk assessment and analysis, and assign to each goal the appropriate level of criticality. The "low-medium-high" set of values is widely used in the risk management practice and declared in the ISO/IEC 270005:2011 as a scale for the description of the magnitude of a potential consequences of a security breach [116]. In this thesis, the prioritisation of security goals means that each goal is assigned the criticality of the range "low-medium-high". The methodology for assigning criticality to security goals is out of the scope of this thesis and one of the existing ones that better suits the organisation using the RMIAS may be adopted (e.g. [117, 118]).

Table 3.1: The IAS-octave

Security Goal Name and Definition	*Analysed Literature*
Accountability - An ability of a system to hold users responsible for their actions (e.g. misuse of information)	[56, 55, 119, 120]
Auditability - An ability of a system to conduct persistent, non-bypassable monitoring of all actions performed by humans or machines within the system	[121, 115, 122, 123, 124, 125]
Authenticity/Trustworthiness - An ability of a system to verify identity and establish trust in a third party and in information it provides	[66, 56, 126, 55, 122, 49]
Availability - A system should ensure that all system's components are available and operational when they are required by authorised users	[65, 66, 86, 56, 55, 122]
Confidentiality - A system should ensure that only authorised users access information	[65, 66, 86, 55, 49, 114]
Integrity - A system should ensure completeness, accuracy and absence of unauthorised modifications in all its components	[65, 66, 86, 56, 55, 122]
Non-repudiation - An ability of a system to prove (with legal validity) occurrence/non-occurrence of an event or participation/non-participation of a party in an event	[56, 55, 122, 49, 14, 127]
Privacy - A system should obey privacy legislation and it should enable individuals to control, where feasible, their personal information (user-involvement)	[128, 61, 45, 129, 130, 131, 132, 133, 134]

As pointed out in Section 2.8.3, one of the shortcomings of the existing literature with regard to security goals is the lack of clarity about which component of an IS each goal is applicable to. In order to remedy this issue in the RMIAS, Table 3.2 shows the applicability of security goals to the components of an IS. The applicability is further explained in the following subsections where security goals are individually discussed.

Table 3.2: The applicability of security goals to the components of an IS

	Components of an IS					
Security Goal	Information	People	Processes	Hardware	Software	Networks
Accountability		X				
Auditability	X	X	X	X	X	X
Authenticity/Trustworthiness	X	X	X	X	X	X
Availability	X	X	X	X	X	X
Confidentiality	X					
Integrity	X	X	X	X	X	X
Non-repudiation	X		X			
Privacy	X	X				

The overlap between goals to a certain degree is unavoidable because the breach of one goal is linked with the breach of another goal. For example, in order to breach the integrity of information, in some cases, the confidentiality of the information must be first breached (i.e. before an unauthorised user may alter information, he/she must gain access to the information). The IAS-octave is an attempt to find a fair balance between too many and too few goals in terms of the level of the categorisation depth (it is often possible to segregate additional sub-goals). Having too many goals leads to unnecessary work complication as too many scenarios have to be considered, but having too few goals may lead to the overlooking of security threats. In the context of IAS, the latter is considered to be more dangerous. An example is provided at the end of Section A.6.0.0.2 in Appendix A.6.

The explicit acknowledgement of additional to the CIA-triad goals is intended to simplify and expedite the understanding of security issues and possible threats, which do not become immediately apparent from the CIA-triad alone, by a non-security audience.

3.7 Security Countermeasures Dimension

*A **Security Countermeasure** is a technique or a process which helps to achieve one or more security goals and helps to mitigate risks to information and vulnerabilities in an IS.*

As discussed in Chapter 2, security countermeasures appear nearly in every conceptual model of IAS. Multiple studies have shown that technical countermeasures alone are not capable of addressing many security-related issues and that a comprehensive approach to security is required [135]. A comprehensive approach means that countermeasures of different nature should be exploited for information protection [54]. The explicit acknowledgement of the variety of available security countermeasures in the RMIAS promotes an holistic approach to security.

Drawing on the analysis of the literature summarised in Chapter 2, the fourth dimension of the RMIAS (left bottom quadrant) demarcates four types of security countermeasures:

1. Technical security countermeasures - the technical means which are exploited to achieve security goals (e.g. cryptography, encryption etc);
2. Organisational security countermeasures - the administrative activities which help to build and maintain the environment where selected security countermeasures may be effectively implemented, managed and monitored (e.g. governance, audit, etc);

3. Human-oriented security countermeasures - the activities which deal with the impact of the human-factor on IAS (e.g. eduction, motivation etc); and

4. Legal security countermeasures - legislation and contractual agreements which protect information (e.g. confidentiality agreement etc).

More detailed description of these four types of security countermeasures along with more extensive lists of examples for each type are contained in Appendix A.7.

These four types cover all security countermeasures were encountered throughout the literature analysis. Only two models (Dark and Harter [89] and Trček [87]) among the examined ones address all four types of countermeasures. The analysed literature does not indicate the existence of another type of security countermeasures apart from the four named above.

The RMIAS incorporates only the high level of abstraction categorisation of security countermeasures. This categorisation highlights the heterogeneous nature of IAS, but at the same time is concise. It is hypothesised to be complete and sufficient for the target audience of the RMIAS. This is tested in the next chapter, where IAS practitioners are interviewed about the RMIAS.

The lists of security countermeasures, which are outline in Appendix A.7, are by no means exhaustive and are only intended to explain the nature of a security countermeasures type. It is beyond the scope of this thesis to produce the detailed taxonomies within each type mainly because this level of detail is unnecessary for the target audience of the RMIAS.

3.8 Interrelationships between the Dimensions and IAS Drivers

In Figure 3.1, the arrows depict the logical dependences between the dimensions of the RMIAS and provide instructions on the use of the model. The RMIAS also captures the drivers that impel IAS decisions: completeness, risk analysis, cost-effectiveness and efficiency, and consistency.

The description of the interrelationships between the dimensions of the RMIAS starts from the top left quadrant and moves clock-wise. An organisation defines its current stage of the security development life cycle and then goes over the other three dimensions to come back to the next stage of the life cycle. It shall be noted that the model does not assume that the security development life cycle should be completed before moving to the next dimension.

For example, an organisation aims to employ the RMIAS for structuring its IAS approach and for the development of a security policy document. Prior to using the RMIAS, the organisation adjusts the model according to its specifics as explained in Section 3.3. The example of the use of the RMIAS and its adaptation for a specific organisation is outlined in Section 3.9.

The organisation identifies that it is currently at the stage of requirements engineering (the Security Development Life Cycle dimension). Then, the organisation moves to the Information Taxonomy dimension. At the stage of requirements engineering, the organisation uses the taxonomy in order to inventory its information assets. The organisation develops a list of information categories[8] it has. After the inventory of information categories is created, the organisation moves to the Security Goals dimension and uses it to establish and prioritise security goals for each category of information. Thus, the organisation identifies and prioritises security goals for each piece of information based on its attributes: form, state, sensitivity and location. Then, the organisation moves to the Security Countermeasures dimension and chooses security countermeasure that may assist in achieving security goals, which were identified earlier, for each category of information. The full cycle around four dimensions of the RMIAS is completed. At the end of this cycle, the organisation produces an Information Security Policy Document (ISPD). The development of an ISPD is discussed in greater detail in the next section.

The organisation now returns to the Security Development Life Cycle dimension. By now, the organisation completed engineering its security requirements and has them formulated in a form of a security policy document. The organisation is now at the stage of security design. At this stage, the organisation again moves around the remaining three dimensions of the RMIAS and ensures that all information assets, security goals and security measures, identified at the previous iteration, are consistently incorporated into and addressed by the system models. The second cycle around the RMIAS is completed.

At the stages of implementation and management/monitoring, the organisation ensures that (1) the established security goals are achieved for every category of information, and (2) all countermeasures are implemented and function as designed.

Thus, in the RMIAS an organisation moves from one stage of the security development life cycle to another, and at each stage of the life cycle it refers to the other three dimensions to identify/conduct actions required at each stage.

[8] Section 3.5.5 explains what information category is.

Further, the explanation of each arrow in Figure 3.1 and the drivers behind the IAS decisions, which are states under the arrows, is provided.

Again the description starts from the top left quadrant. The top arrow declares that starting from the first stage of the security life cycle every category of information, encountered in a specific organisation, must be identified. An organisation inventories thoroughly all information it has. Section 3.9 demonstrates how an inventory of information may be created using the RMIAS. The use of the information taxonomy for cataloguing information which requires protection guarantees higher ***completeness*** of an ISPD. The ***completeness*** on an ISPD is further ensured by the consideration of all relevant security goals for every identified category of information.

Not all goals are equally important for every category of information. The right arrow shows that for each category of information an organisation prioritises security goals driven by ***risk analysis***. The RMIAS is not a risk analysis or risk assessment methodology and it does not provide a tool for prioritising security goals. However, the RMIAS points out the important place of risk analysis in the IAS domain and articulates the requirements towards a risk analysis methodology which should (a) assist with the creation of a detailed inventory of information and (b) facilitate the prioritisation of security goals.

After the cataloguing of information and the prioritisation of security goals, an organisation identifies the countermeasures that help it to achieve established goals. The bottom arrow shows that the choice of countermeasures is driven by ***cost-effectiveness*** and ***efficiency***. An organisation does not aim to eliminate risks and protect information at any price, but to mitigate them to an acceptable level and only in the most cost-effective way ensuring that the chosen countermeasures do not hinder each others efficiency. The consideration of the full spectrum of security goals, supported by risk analysis, enables the development of the optimum (cost-effective and efficient) combination of security countermeasures.

The left arrow illustrates that the selected security countermeasures should be traced with ***consistency*** throughout all stages of the security development life cycle. The circle created by the arrows shows that the model should be used in iterations at every stage of the security development life cycle. For example, if at the stage of requirements engineering it is identified that the personnel should use the information classification scheme, then at the design stage (1) the provision of training on the classification scheme should be embedded into business process models to guarantee that the required time and resources are allocated and (2) the training materials should be developed. At the implementation stage the actual training should take place and its effectiveness

should be checked by knowledge tests. At the stage of management/monitoring the correct use of the classification scheme should be monitored. The scheme should be updated when necessary to reflect changing business circumstances and employees should be retrained if required.

If any change in either dimension should occur, the RMIAS should be updated accordingly and all steps should be repeated, e.g. if an organisation plans to allow employees to work from home, in the information taxonomy dimension a new possible value "*employees' homes*" should be added to the attribute location, and for the new categories of information, where L="*employees' homes*", security goals should be prioritised and appropriate countermeasures selected.

3.9 Use of the RMIAS

In addition to the descriptive knowledge, which is described in Sections 3.3-3.8, the RMIAS also embeds the methodological knowledge[9]. This section explains how the RMIAS may assist with the development of an ISPD.

There is a hierarchy of security policies, where each policy document addresses security at a different level of detail [137, 138].

Further in the thesis, an ISPD refers to a governing policy document which specifies what security goals should be achieved and what security countermeasures should be put in place at a high level of abstraction leaving more precise details for the supporting documents (e.g. technical policies, job aids and guidances) [81, 138]. The detailed description of an ISPD and its content is given in ISO/IEC 27002:2005, Sec 5.1 [69].

An ISPD consists of a number of statements[10]. Below are the examples of security policy statements:

1) To ensure integrity and confidentiality, all backup data must be encrypted.

2) To ensure confidentiality and accountability, sensitive documents may be taken out of the office only with the permission of senior management.

[9]The descriptive knowledge - "knowledge that" - accumulates assertions about the world, while the methodological knowledge - "knowledge how" - outlines instructions for conducting actions [136]

[10]In the context of InfoSec management the term "information security policy statement" is usually used. In the system engineering context the similar type of statements is often referred to as system or security requirements.

A security policy statement does not typically provide the full details (e.g. what software or hardware should be used to encrypt data or who is the person responsible for signing permissions for taking documents out) [138]. This level of abstraction is sufficient for and accessible by the target audience of the RMIAS (i.e. when discussing IAS issues a multi-disciplinary team does not typically require to know about encryption algorithms to be used or the details of the legal agreement with a third party and the like; these details may be dealt with by a domain expert).

As partially discussed in the previous section, in the RMIAS, an element of one dimension is combined with an element of each other dimension in order to create a comprehensive list of situations in which information needs protection. This ensures that a security policy statement exists for each situation.

The use of the RMIAS is demonstrated in this section using the example of Translate, the SME which was introduced in Section 3.5.2.

First, the RMIAS is adapted for the specifics of Translate. In the Information Taxonomy dimension, the location and sensitivity classifications which are in use by Translate are added to the model. Figure 3.5 depicts the RMIAS as adapted for use by Translate. The elements of the Information Taxonomy, which are specific to Translate and are added to the model as such, are depicted in bold (the levels of information sensitivity and the categorisation of locations). Information of all three forms is dealt with by Translate and, therefore, all three forms are kept in the model. The security requirements engineering stage in the security development life cycle dimension is also shown in bold to highlight that Translate is currently at the stage of requirements engineering. In this example, the element of the security development life cycle dimensions is fixed at the requirements engineering stage. Translate adopted the IAS-octave as a set of security goals. At this stage, the elements of the other three dimensions are combined to produce an ISPD.

The format of a table provides a convenient way for combining the elements of the three dimensions of the RMIAS. Table 3.3 has six columns: form, sensitivity, location, state, security goal and security countermeasure type & description. The table is populated with all possible combinations of values of the following attributes: form, sensitivity, location, state and security goal. At this stage, the last column - security countermeasure type & description - is left empty.

The number of all possible combinations of the categories of information and security goals (which

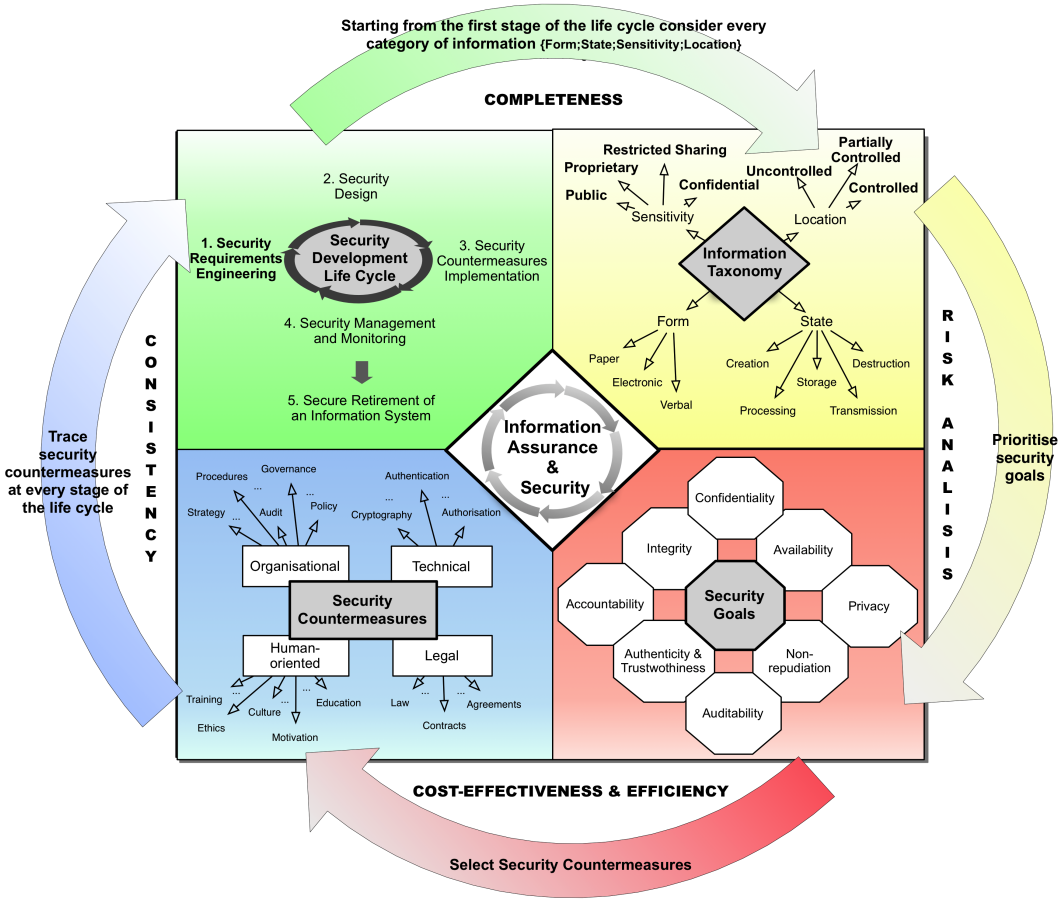


Figure 3.5: The RMIAS as adapted for Translate

is also the number of rows in the table) is calculated as follows:

$$N = N_f * N_s * N_{sen} * N_l * N_{SG}, \tag{3.1}$$

where

- N - the number of possible combinations of the categories of information and security goals,
- N_f - the number of the forms of information,
- N_s - the number of the states of information,
- N_{sen} - the number of the levels of information sensitivity,
- N_l - the number of locations, and
- N_{SG} - the number of security goals.

For Translate, the number of rows in the table is equal to

$$3 * 5 * 4 * 3 * 8 = 1440, \tag{3.2}$$

where

- 3 - the number of the forms of information (paper, electronic and verbal),
- 5 - the number of the states of information (creation, processing, storage, transmission and destruction),
- 4 - the number of the levels of information sensitivity (*Confidential*, *Restricted Sharing*, *Proprietary* and *Public*),
- 3 - the number of locations (controlled, partially controlled and uncontrolled),
- 8 - the number of security goals (the IAS-octave), and
- 1440 - the number of possible combinations of the categories of information and security goals,

Thus, each row (i.e. each combination of a category of information and a security goal) in the populated table refers to a particular scenario or rather a group of scenarios in which the information of that category may need protection from threats covered by the referenced security goal.

For example, row 1 in Table 3.3 refers to privacy of paper documents which are classified as *Public* and processed in an uncontrolled environment (e.g. an advertisement brochure is read by a prospective client).

Row 2 refers to the non-repudiation of information which is contained in electronic documents classified as *Public* and stored in a controlled environment (e.g. a video-press release of Translate which is stored on the company's server).

Then, Translate considers each row in the table (i.e. each combination of the elements of the RMIAS). For each row, Translate establishes how critical the security goal is for the category of information. If Translate decides that the violation scenarios outlined by the row are realistic and pose threat to the organisation then actions should be taken to achieve the security goal for the category of information. A decision is then made on which security countermeasures must be put in place for the prevention of the scenario. A multi-disciplinary team of experts may be involved in this discussion.

Table 3.3: The development of an Information Security Policy Document for Translate using the RMIAS.

	1. Form	**2. Sensitivity**	**3. Location**	**4. State**	**5. Security Goal**	**6. Security Countermeasure Type: Description**
1	Paper	Public	Uncontrolled	Processing	Privacy	Not required.
2	Electronic	Public	Controlled	Storage	Non-repudiation	Not required.
3	Electronic	Public	Controlled	Storage	Availability	Technical: All electronic information must be backed up every night (Backup on an external hard drive and using an online backup service).
4	Paper	Confidential	Controlled	Storage	Confidentiality	Organisational: Store in a safe and ensure that only authorised personnel have access to the safe.
5	Paper	Confidential	Uncontrolled	Transmission	Confidentiality	Organisational: Documents must not be taken out of the office.
6	Paper	Proprietary	Controlled	Processing	Accountability	Organisational: Access to all proprietary documents must be logged. Legal: Non-disclosure agreement must be sighed by all members of staff granted access to proprietary information.

The number of possible combinations of information categories and security goals, as calculated above (Formula 3.2), is substantial. However, not each possible combination (row in the table) is applicable in the context of a specific organisation. Consequently, security countermeasures and, as a result, security statements in an ISPD are required not for every combination. Nevertheless, it is critical to identify (and keep them in the table) all potential situations in which information needs protection, and then consciously mark irrelevant ones as such. It ensures that no potential security violations is overlooked, and enables the traceability and defensibility of security decisions.

In row 1 of Table 3.3, no security countermeasures are required to protect privacy of a *Public* document as there are no such scenarios in which privacy may be violated by misusing a *Public* document. Hence, for this combination no security policy statement is developed. Similarly, in row 2, the non-repudiation of a *Public* document poses no threats to Translate and this combination of attributes and the security goal is excluded from further consideration. However, while non-repudiation is not critical for a *Public* electronic document located in a controlled environment,

availability is. The scenarios in which the availability of a *Public* electronic document located in a controlled environment may be breached may be as follows: (1) an employee deletes the document by mistake, (2) the physical damage of the server on which the document is stored (e.g. due to fire or flood), (3) the external host of the document does not provide access to the document in violation of a service agreement, etc. Row 3 specifies that the availability of the electronic documents, which are classified as *Public* and stored in a controlled location, must be ensured by means of creating backups both on an external hard drive and in the cloud using one of online backup services.

Row 4 contains a security policy statement which dictates that for the *Confidential* paper documents which are stored in a controlled location (e.g. printed financial and audit reports stored in Translate's office) an organisational security countermeasures should be put in place, namely, the documents must be stored in a locked safe and it must be ensured that only authorised personnel have access to the safe. Row 5 declares that *Confidential* paper documents cannot be transmitted to an uncontrolled environment.

Row 6 refers to the accountability for the use/misuse of information classified as proprietary while it is being processed in the paper form in a controlled location. To achieve accountability the access to *Proprietary* paper documents must be logged (organisational security countermeasure) and non-disclosure agreements must be in place with every employee of Translate who has access to the information classified as *Proprietary* (legal security countermeasure).

The above discussed examples of security policy statements, which are summarised in Table 3.3, are sufficient for the purpose of demonstrating how an ISPD may be developed based on the RMIAS. The consideration of all possible situations in which information needs protection (i.e. all possible combinations of the parameters form, location, state, sensitivity and security goal) for Translate is beyond the scope of this thesis.

This section demonstrated that the RMIAS provides a tool for identifying more situations in which information may need protection than other models may assist with identifying. By doing so, the RMIAS guarantees the higher completeness of an ISPD.

3.10 Visual Appearance of the RMIAS

The decision to develop a clear visual representation for the RMIAS was guided by the following considerations. Visuals increase the willingness to read by 80% [139]. People remember visually presented information better than a text [140].

The RMIAS is depicted in a notation-free form. However, some elements of knowledge representation technique such as mind map may be observed in it. Mind map is one of the best known techniques for the organisation of knowledge; it assists with problem/topic understanding and problem solving, and facilitates communication regarding the topic [141].

The use of colour in the RMIAS enhances the model comprehension. However, in the RMIAS colour is employed in a redundant way. Hence, the RMIAS when it is presented in a black-and-white mode does not loose any information.

The choice of the colour for each dimension is driven by the following associations:

- The green colour of the security development life cycle dimension. Association: in a traffic light the green colour permits movement ("Go" command) and is associated with motion.
- The yellow colour of the information taxonomy dimension. Association: in a traffic light the yellow colour indicates "Be Prepared" command. Information profiling and cataloguing promotes the preparedness of an organisation for the protection of information.
- The red colour of the security goals dimension. Association: in a traffic light the red colour indicates "Stop" command. Red is also the colour of danger in Western cultures. Security goals prompt an organisation to "stop" and consider threats to information.
- The blue colour of the security countermeasures dimension. Rationale: in ISO 7010:2011(E) M001 *Graphical symbols. Safety colours and safety signs. Registered safety signs* [142], blue is the colour of compulsory action signs. Blue colour is associated with "Do" command.

In the RMIAS, different geometrical shapes depict different IAS concepts in order to increase perceptual discriminability:

- The security development life cycle dimension - circle or oval (association with a cycle);

- The information taxonomy dimension - rhombus (four sides of a rhombus point out to four attributes of information),
- The security goals dimension - octagon (eight angles of an octagon point out to eight security goals in the IAS-octave). The modular structure, as inspired by [30], is adopted for the visualisation of the IAS-octave. It highlights the fact that the set of security goals is not fixed, and must be regularly revised to reflect changes in an environment and extended when needed; and
- The security countermeasure dimension - square (four angles of a square point out to four types of security countermeasures).

3.11 Concepts which are not Explicit in the RMIAS

The RMIAS brings into a sharp focus some concepts of the IAS domain and blurs the others. In the description of each dimension, the explanation is given on why a particular concept is important in the IAS domain and why it is included in the RMIAS. This section presents a discussion of the IAS concepts which are not explicitly depicted in the RMIAS. This section aims to provide the justification for non-inclusion of the concepts discussed below. While working on the RMIAS, the Ockham's razor principle was followed which promotes parsimony, economy, or succinctness in problem-solving and states that entities must not be multiplied without a necessity and that the simpler explanation is to be preferred [143].

Assets Classification. One question, which may arise with regard to the RMIAS, is why among all assets that need protection the model considers only information (the information taxonomy dimension). One may argue that all six components of an IS, which according to Definition 4 are (1) information (data), (2) people, (3) business processes (procedures), (4) hardware (5) software and (6) networks, should be included in the model as the objects of protection. This approach is logical. However, the primary objective of IAS is the protection of information. Other components of an IS are protected in order to achieve the primary goal, but not for their own sake. This is captured in the InfoSec definition which is adopted in this thesis (Definition 1).

Furthermore, considering the protection of every component of an IS in one model will make the model over-complex and, therefore, harder to comprehend. The introduction of such complexity

is deemed unnecessary for the target audience of the RMIAS.

Threats Classification. There are two approaches to analysing IAS issues [58]: threat-based and goal-based approaches. The threat-based approach analyses specific threats to information and works out the security solution based on this analysis. The goal-based approach operates at a higher level of abstraction. A security goal corresponds to a specific category of threats [126]. Rather than focusing on a specific threat or malicious act, a security goal refer to an entire category of threats that fall under the same description.

Focusing on goals allows security experts to communicate with stakeholders and business experts using concepts that do not require technical knowledge and are accessible to a non-technical audience [144]. Further advantages of the goal-based approach, as discussed in [58], are as follows:

- It does not heavily rely on statistics, which are difficult to acquire. The goal-based approach relies more on expert's judgement. On the contrary, for threat-based risk analysis, statistics are crucial;
- It is more accessible to management and other non-technical staff, whereas threat analysis requires technical knowledge;
- It captures the essence of the problem and exposes it at a higher level of abstraction, where as the threat-oriented approach goes into greater detail;
- It achieves greater completeness, while completeness of the threat-based approach primarily depends on the expertise of an analyst; and
- It is an inherent human inclination to set goals for activities.

Since the RMIAS is designed for a wide audience, including non-technical experts, the use of the goal-based approach is preferred.

Risk. Risk is one of the important concepts in IAS. In the RMIAS, the importance of risk is acknowledged in two ways. First, risk analysis is carried out as a part of the requirements engineering stage of the security development life cycle (Appendix A.4, Table 2). Second, risk analysis is declared as the driver which guides the prioritisation of security goals. Based on the business specifics, an organisation defines the level of criticality for each security goal and decides on the

investments it is prepared to undertake on the achievement of the goal. Thus, in the RMIAS the nature of risk is conveyed via the type of a security goal and the severity of risk via the criticality of a security goal.

3.12 Discussion

3.12.1 The RMIAS as an Abstraction

In resemblance with the famous story of the Indian subcontinent about men in darkness and an elephant[11], IAS means different things to different people. The RMIAS presents only one possible viewpoint on IAS. Although acknowledging that the RMIAS is not the only way to convey IAS knowledge, it is argued to be the most suitable for the purpose of this research and the outlined targeted audience due to the chosen form of representation (Section 3.2), the included set of concepts and the level of detail (Section 3.1).

IAS is a heterogeneous and complex domain. Attempting a large topic as capturing the IAS domain knowledge, no model of IAS might be absolutely comprehensive or impartial because (1) omissions are inevitable in order to deal with the complexity of the domain, (2) any author is biased by his/her background knowledge, experience and perspective, and (3) a model is designed for a specific purpose and audience.

Any model is a surrogate for the object being represented and "complete accuracy" is, by definition, unachievable [104]. Fidelity is only required to the level to enable the usability of a model for an intended purpose. The RMIAS, as with any other reference model, sacrifices some details in order to show the full breadth and complexity of the modelled domain. An attempt to cover the entire knowledge area forces decisions to be taken that may launch a polemic. To address this, this chapter made the decisions taken while developing the RMIAS (e.g. the use of a reference model as the form of knowledge representation, the choice of concepts to be included in the RMIAS) transparent and supported by argument.

The RMIAS is designed for communicating IAS concepts to business experts and other non-technical audiences. The purpose and the target audience of the RMIAS influenced the choice

[11] A group of men in darkness touch an elephant to learn what it is. Each man feels a different part, but only one part of an elephant. After comparing their notes they learn that they are in complete disagreement on what an elephant is [145].

of concepts to be included in the RMIAS as well as the choice of the form of knowledge representation. To suit its target audience, the RMIAS operates at the level of high abstraction ignoring precise (e.g. technical, legal or other) details with which a non-technical, non-security and business audience may be unfamiliar.

The RMIAS is generic as any reference model should be. It attempts to cover the aspects of IAS which are relevant to the majority of organisations. This implies that the RMIAS requires an adaptation when being applied in the context of a specific organisation. To facilitate this the RMIAS is flexible and allows organisation-specific adjustments as discussed in the previous sections.

Furthermore, the structure of the RMIAS is flexible to allow extensions which may be required due to changes in an environment, society and technology. The existing dimensions may be extended (new security goals, new types of security countermeasures may be added to the RMIAS, the information taxonomy may be extended) and even new dimensions may be introduced.

The RMIAS prompts its users to consider aspects of IAS which are critical and must be addressed. However, the RMIAS does not provide direct answers or solutions to security issues, it rather points out to the questions to be asked and assists with thinking about IAS.

3.12.2 Implications of the RMIAS

In the subsequent chapters of this thesis, the RMIAS is used as a basis for the semantics of an extension for a business process modelling language. However, while developing the RMIAS, the IAS domain was considered in all its breadth and was not constrained to the business process view only.

On the contrary, an attempt was made to understand and capture IAS domain as it is understood by IAS professionals and academics and, then, bring this conception of IAS into business process models. The solid foundation the RMIAS builds upon allows making a prediction of its usefulness in many other areas. The implications of the RMIAS for education, research and practice are enumerated below:

Education -

1. Provides a framework for teaching IAS topics (development and structuring of educational programs);

2. Promotes faster familiarisation with the IAS domain;

3. Fosters seeing a "big picture" of the IAS domain.

   Throughout this project, it was often encountered that InfoSec technical experts, who concentrate on one specific technical security countermeasure, believe that it solves all security issues. It was also noted, that some IT security students also suffer from this faulty approach to IAS. However, the understanding of the technological aspect of information protection or of one technical security countermeasure (e.g. cryptography or firewall) will be incomplete without understanding the context in which these technologies are applied [8];

4. Assists with the communication of the meaning and scope of IAS to an audience outside the IAS community;

Research -

5. Structures the IAS knowledge-base acquired by researchers and practitioners;

6. Provides a framework for cataloguing existing InfoSec and IA research and helps to identify the place of a particular topic of interest in the domain;

7. In conjunction with literature analysis, may point out gaps in the research;

Practice -

8. Provides a system for organising security thinking and practice in an organisation;

9. Plays the role of a framework for the design, implementation and assessment of a secure IS; and

10. Facilitates communication with regard to IAS issues between stakeholders.

Chapter 4 is devoted to the evaluation of the RMIAS where it is demonstrated how well the RMIAS fulfils some of the above enumerated roles. In Chapter 4, it is also discussed how the IAS practitioners, who were involved in the evaluation of the RMIAS, appraise the implications of the RMIAS for different areas.

3.13 Chapter Summary

One of the research objectives of this research project, as declared in Section 1.3, is *to develop an up-to-date conceptual model of IAS suitable for the wide audience including experts with different backgrounds* (Objective 1.B). In this chapter, the RMIAS is introduced to achieve this objective.

The problem addressed in this thesis is declared as follows: an understanding of the IAS domain shared among the members of a multidisciplinary team must be achieved prior to the discussion of IAS issues and prior to the security-annotation of business process models (Section 1.2). The RMIAS solves this problem because it reflects a common understanding of IAS as it is presented in the literature. It may be exploited by a multidisciplinary team for harmonising their understanding of the domain and may serve as the basis for the semantics of an IAS modelling language.

The RMIAS is pre-validated, at least to a certain degree, since it was developed as a synthesis of the existing models of InfoSec and IA, and the existing knowledge of the IAS domain. The novelty of the RMIAS is in the combination of the discrete knowledge with the purpose to draw an holistic picture of the IAS domain.

In the next chapter, the RMIAS is evaluated with regard to how well it meets the quality criteria of a conceptual model. It is tested to what degree the RMIAS reflects the comprehension of the IAS domain of the IAS practitioners and academics being interviewed. The pragmatic value of the RMIAS is also validated in the next chapter via the workshops with MSc students studying IAS-relevant programs and via a case study.

Chapter 4

Evaluation of the RMIAS

Section 1.3 declared that one of the objectives of this thesis is to evaluate the proposed solution. This chapter is devoted to the evaluation of the RMIAS and tests Hypothesis B (Section 1.4). First, this section outlines the multiphase evaluation methodology and justifies the choice of the evaluation criteria. Next, it analytically evaluates the RMIAS, analyses the responses of the interviewees as well as the feedback from the workshops and the case study. Finally, the RMIAS is compared with other conceptual models of the IAS domain. The chapter concludes with the discussion of the evaluation results.

4.1 Evaluation Methodology

The evaluation of a conceptual model is an arduous task due to the lack of a rigorous basis for evaluation: "*a conceptual model exists only as a construction of the mind, and therefore quality cannot be as easily assessed*" [99]. Clear methods for the evaluation of conceptual models are still lacking and evaluation is often subjective and/or hard to formalise [99].

In this thesis, a multiphase evaluation route was designed and pursued in order to test Hypothesis B[1] and demonstrate the merits of the RMIAS in a valid sustainable way. A conceptual model may be evaluated analytically and empirically. The discussion of these two types of evaluation and their limitations is presented in Appendix A.8. Each proposed evaluation method has its

[1]Hypothesis B: The RMIAS provides more complete and accurate representation of the IAS domain, than the existing conceptual models of the IAS domain. The RMIAS reflects how the IAS domain is understood by IAS domain experts and represents the domain in the form accessible by the experts with the different backgrounds and with the different levels of experience in IAS. Due to the above, the RMIAS helps to build a congruous understanding of the IAS domain in a multidisciplinary team of experts and provides a solid basis for the semantics of Secure*BPMN (Section 1.4).

limitations [146, 147]. Therefore, a combination of different evaluation methods was exploited to overcome the limitations of separate methods.

The multiphase evaluation of the RMIAS is intended to verify both the scientific value and pragmatic value of the RMIAS by combining the following methods of evaluation:

- To test the scientific value:
  - (1) *A solid theoretical basis;*
  - (2) *Analytical evaluation by the model developer;*
  - (3) *Interviews with academic and industry IAS experts;*
- To test the practical value (utility):
  - (4) *Workshops with MSc students and IAS practitioners;* and
  - (5) *Case study.*

Figure 4.1 schematically depicts the RMIAS evaluation methodology.

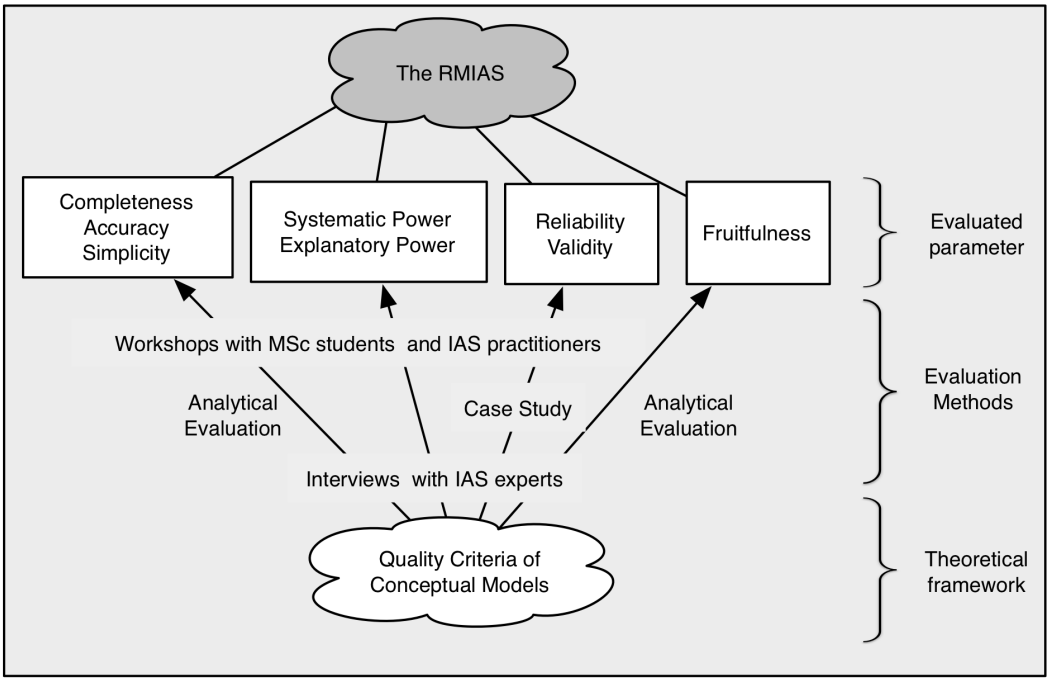


Figure 4.1: The evaluation of the RMIAS. Excerpt from Figure 1.2.

The scientific value (truthfulness) of the RMIAS is, at least to some degree, justified by the IAS literature it draws upon. As manifested by the references cited in Chapter 3, there are research and/or industry publications related to each element of the RMIAS.

Since this justification is not deemed to be sufficient, to prove the scientific value of the RMIAS further, the model is evaluated analytically by the model developer for its compliance with the quality criteria of conceptual models. This criteria are introduced in Section 4.1.1, where the choice of the criteria is also justified. In Section 4.5, the RMIAS is also compared with other IAS conceptual models and it is analytically demonstrated that the RMIAS outweighs the other models in terms of completeness and accuracy. The developer possesses the in-depth understanding of the model and is well equipped to perform analytical evaluation. However, such evaluation is subjective because the developer is inevitably inclined towards her proposal. Furthermore, the evaluation results are unavoidably affected by the perspective and background of the evaluator.

In order to complement and address the limitations of the analytical evaluation mentioned above, a series of semi-structured interviews[2] with IAS experts, who are impartial towards the model, was conducted to apprise the quality of the RMIAS. The interviews aimed to test how well the RMIAS corresponds with the experts' understanding of the IAS domain and how well it complies with the quality criteria of conceptual models (Section 4.1.1), according to the opinion of the experts. Testing Hypothesis B (Section 1.4), it was also examined whether the RMIAS represents the domain in the form accessible by the experts with the different backgrounds and with the different levels of experience in IAS.

For the validation of the methodological knowledge of the RMIAS it was essential to empirically demonstrate the practical value of the model [30]. The practical value of the RMIAS (i.e. how viable and useful the model is in practice) was tested via the workshops with MSc students and IAS practitioners and via a case study[3].

[2]Semi-structured interview is an interview, run by a researcher, where there is a script which covers some questions and helps to keep the focus of the discussion, but there is still a room for openness, flexibility and improvisation [146].

[3]A similar evaluation approach can be found in [148], where the framework for dealing with non-functional requirements is evaluated analytically by its developers and then additional evidence is provided by case studies and interviews with domain experts. The important roles of case studies and interviews in IS research and, particularly, in qualitative IS research are discussed in [147] and [146] respectively

4.1.1 Evaluation Criteria

There are multiple proposals, originating both from research and practice, suggesting methods for the evaluation of the quality of conceptual models. In [99], at least fifty proposals are identified and analysed.

Many evaluation frameworks agree on the need for a multi-criteria approach. In [149], six criteria are suggested: simplicity, understandability, flexibility, completeness, integration and implementability. In [12], three basic guidelines for high quality conceptual models (correctness, relevance and economic efficiency) and three optional guidelines (clarity, comparability and systematic design) are proposed.

For the evaluation of the RMIAS the criteria, which are suggested in [33] and further elaborated in [27], are adopted:

1. **Simplicity** - among models, equal in other ways, preference is given to the simpler model;
2. **Accuracy** - a model as well as the concepts it incorporates should be accurate and explicit;
3. **Scope (Completeness)** - a model should cover the broader scope of a modelled domain and should not overlook essential concepts;
4. **Systematic power** - a model should help to organise concepts and relationships between them in a meaningful systematic way;
5. **Explanatory power** - a model should assist with explaining and predicting a phenomena;
6. **Reliability** - a model should be valid in all situations for which it is designed and should lead to similar understanding when applied to the same phenomenon by different users;
7. **Validity** - a model should provide valid representations and findings; and
8. **Fruitfulness** - desirably a model should suggest research problems and hypotheses for testing.

The choice of the evaluation criteria suggested in [33] is driven by the following considerations:

- Purpose: These criteria are specifically destined for the evaluation of a conceptual model of an area of research (i.e. a reference model), while criteria proposed in [149] are designed for

the evaluation of Entity Relationship Models and the guidelines in [12], for the evaluation of business process models.

- Application: These criteria are applied to the evaluation of information seeking and retrieval research by the authors of the criteria [33]. The criteria are also exploited for the evaluation of a definition of an IS [27], independently of the authors of the criteria. Other evaluation frameworks present only a theoretical basis, but do not provide any application examples.

- Completeness: The set of quality criteria is more comprehensive than the sets of the quality characteristics found in other proposals.

The RMIAS was analytically evaluated against these eight criteria by the model developer and by the IAS experts who were interviewed. The workshops and the case study contributed the evaluation of the RMIAS with regard to reliability and validity. The arrangements of interviews, workshops and case study are outlined as well as the evaluation results are discussed further in this chapter.

4.2 Analytical Evaluation and Analysis of the Interviews

Sections 4.2.1 - 4.2.8 present discussions on how the RMIAS addresses each of the eight quality criteria chosen.

The first part of sections 4.2.1 - 4.2.8 outlines the comments of the author related to a particular criteria. These sections also draw a link between this chapter and Chapter 2, and make the comparison between the RMIAS and other analysed models of IAS. The last row of Tables 2.5, 2.6 and 2.7 presents the RMIAS for comparison purposes. These tables are discussed further in this chapter. The second part of Sections 4.2.1 - 4.2.8 discusses the comments of the interviewed experts.

Further, this section provides the details of the interviewing process as recommended in [146].

For the interviews, the professionals and academics who have experience in the IAS domain or related areas were targeted. The experts who participated in the evaluation, first, were given an oral presentation which briefly discussed the existing models of IAS and described the RMIAS in detail. Then, the participants challenged the model in a question and answer session. Three out of five presentations were followed by a workshop (the details of the workshops are described in

Section 4.3.1), where the participants had a chance to apply the RMIAS on a case study. Table 4.1 summarises the details of the presentations and workshops.

The interviews were arranged either on the same day following the presentations or, in several cases, at a later date. Each interview lasted between 30 - 60 minutes. At the beginning of an interview, the purpose of an interview was communicated to an interviewee and reassurance was given that in all written work the responses will appear anonymously.

Some responses were received in a written form due to the difficulties of arranging a personal meeting. Two interviewees did not attend the presentation, but filled in the questionnaire based on the written description of the RMIAS as it appears in [96]. These two interviewees filled in the questionnaire and returned it by email.

Table 4.1: RMIAS evaluation presentations and workshops

Date	Venue	Duration	Audience	Participants	Responses
12.11.2012	Cardiff University, the School of Computer Science & Informatics. Informatics Group Seminar	1 hour (presentation)	Academics	9	4
13.12.2013	Cardiff University, group of MSc students	2 hours (presentation and workshop)	MSc Students	8	0
26.02.2013	Cranfield University, Defence Academy, group of MSc students	2 hours (presentation and workshop)	Practitioners and MSc students	13	10
03.04.2013	University of West of England. Software Engineering Research Group	1.5 hours (presentation)	Academics and Practitioners	12	6
24.04.2013	Cardiff University, Information Security Program	3.5 hours (presentation and workshop)	Practitioners	4	4
March 2013	remotely	n/a	Practitioners	n/a	2

To facilitate the interviews, a questionnaire was developed based on the chosen set of evaluation criteria (Section 4.1.1). For each criterion a number of questions was developed. A pilot test of the questionnaire was run with a group of three PhD students and two lecturers, who specialise in InfoSec and Privacy, at the School of Computer Science & Informatics, Cardiff University. The group was familiar with the RMIAS and informed about the objectives of the study. According

to the comments of the pilot-test group, the questionnaire was corrected to enhance its clarity and several questions were dropped as monotonous.

The final version of the questionnaire included fifteen questions. The questionnaire could be found in Appendix A.10. First three questions gathered information about a respondent (the number of years of experience, nature and area of expertise). The remaining questions asked a respondent to evaluate the RMIAS in terms of the chosen quality criteria. The last two questions in the questionnaire related to the fruitfulness of the RMIAS for research. These questions required a respondent to have an academic background in IAS. Therefore, if a respondent had only practical experience in IAS the last two questions were excluded from an interview. The questions, as they were formulated in the questionnaire, are restated in Section 4.2, where the results of the interviews are analysed.

The interviews were semi-structured. The questionnaire provided a template for the discussion, but the participants were invited to give extended answers and to explain their position. At the end, the respondents were invited to provide any comments that were not captured by the questions. Both the transcripts and notes were used as the recording technique.

All presentations, interviews, workshop and the analysis of the results were carried out by the author. With seven interviewees the interviewer was acquainted as with colleagues prior to the presentation and interviewing procedure, and two of seven interviewees were exposed to the early versions of the RMIAS and knew the details of the development process. Other interviewees the interviewer had not previously met.

Overall, 26 full responses were received over the period between November 2012 and April 2013. The participants profile is presented in Appendix A.11. As Appendix A.11 shows, the experience of the respondents varies from 1 to 32 years with the average of 9.9 years. Among the interviewees there were 5 academics, 15 practitioners and 6 experts whose experience comes from both research and practice. Appendix A.11 further shows that the respondents specialise in the diverse range of the aspects of IAS and in related domains. The profile of the interviewees confirms that the RMIAS was evaluated by the independent experienced audience and that the RMIAS was approached from different perspectives conditioned by the backgrounds of the respondents. Thus, the participants' profile fortifies the quality and trustworthiness of the evaluation results.

The transcripts of all interviews could be found in Appendix A.12. In this section, thick description[4] accompanies the analysis of the interviews to enable the reader to see the genuine responses

[4]While thick description means that verbatim quotations from responses are used, thin description refers

and to minimise misinterpretation.

4.2.1 Simplicity of the RMIAS

Simplicity is a subjective characteristic: what is simple for one individual, may be complex for another. Objectively, simplicity may be analytically evaluated against other models. In comparison with other models (e.g. McCumber's cube [65], Maconachy et al. [86]), the RMIAS is more complex. The RMIAS has a wider scope than other models and, therefore, it inevitably has more elements and is less simple. However, according to the Ockham's razor principle [143], the simple explanation or model should only be preferred until simplicity can be traded for greater explanatory power. It may be hypothesised that the RMIAS has greater explanatory power than the other models because it may represent more security issues and solutions, and it also makes the interrelationships between the IAS concepts explicit. This statement is supported by the analysis of the other models summarised in Tables 2.6 and 2.7 which show that none other of the examined models covers the same range of security concepts as the RMIAS. The detailed analysis of other models of IAS is presented in Chapter 2.

The RMIAS also attempts to cover the full breadth of the IAS domain. As the result of this, in the trade-off between simplicity and completeness, in the RMIAS, the preference is given to completeness.

Despite being more complex than other analysed models according to the analytical evaluation conducted by the author, the RMIAS is considered as relatively simple and easy to grasp by the interviewed experts and even by newcomers to the IAS field as discussed in Section 4.3.2. In order to enhance its intelligibility, the RMIAS is duly accompanied by a narrative. The definitions of every element of the RMIAS are provided and the interrelationships between the elements are explained. The visual appearance also aims to improve the intelligibility of the RMIAS. During the workshops, the RMIAS was presented to the audience which had different levels of expertise in IAS. The feedback from the participants indicates that even the novices to IAS find the model simple and easy to understand. As discussed in Section 4.3.2, the novice participants along with more experienced ones successfully used the RMIAS for the development of an ISPD during the evaluation workshops.

to the use of little or no quotations [146].

In the interviews, there were two questions capturing the opinion of interviewees with regard to the simplicity of the RMIAS:

- Question 4 - Are the elements of the RMIAS simple?
- Question 5 - Are the relationships between the elements simple? (The relationships are illustrated by arrows.)

Twenty-two out of twenty-six interviewees described the elements of the RMIAS as simple. The following comments were received for question 4:

Respondent 6: "*They are simple. A very easy way of expressing requirements to key stakeholders*."

Respondent 9: "*The diagram is quite simple, but also conveys a complex depth.*"

Respondent 11: "*Following the explanation, the model is simple. However, its rather comprehensive approach possibly detracts from the optimum level of simplicity*."

Respondent 13 - "*Yes, it appears clear and easy to implement.*"

Respondent 19 - "*Yes. They appear to be simple at the coarse or more abstract level.*"

Respondent 20: "*The elements of model are simple, but the difficulty lies in how to show them (I think!). The model needs to be viewed from other perspectives for identifying its simplicity. I mean that if the model is four dimensional, can I present it as a series of three dimensional projections that progress over the fourth dimension?*."

Respondent 21: "*I think that the model, with regards to the dimensions is fairly simple to understand. I don't think it would be as easy to implement because it will highlight such a high number of risks.*"

Respondent 23: "*Yes, the elements are reasonably self-explanatory and straight forward to understand. One comment I have is that visually the diagram gives the impression that you would complete the contents of each quadrant (so to speak) before moving onto the next. However the security development life cycle is not something you would "complete" before moving onto the information taxonomy dimension. In practice, when carrying out security requirements elicitation you would "Consider every stage of information", "Prioritise security goals", and "Select security countermeasures" before moving to the security design stage in the development life cycle. I am not convinced the development life cycle sits as a quadrant within the diagram and should perhaps sit centrally or outside the diagram. Steps 1,2 and 3 in the security development life cycle*

are informed by information taxonomy, security goals and security countermeasures, so it feels incongruous to have them in a flow."

Thus, although two respondents (respondents 20 and 23) found the elements of the RMIAS simple, they suggested to change the layout and improve the visual effectiveness of the RMIAS. Respondent 23 interprets the role of the security development life cycle in the RMIAS exactly as it is meant, but suggests that the visual appearance of the RMIAS does not convey the view on the life cycle as a time line in the most effective way. In order to eliminate possible misinterpretations of the role of the security dimensions life cycle, the detailed explanation of the role of this dimension and of its interrelationships with other dimensions is presented in the narrative of the RMIAS in Chapter 3.

Respondents 13 and 21, although both agreed that the elements of the RMIAS are simple, had opposite opinions regarding the simplicity of the implementation of the RMIAS.

Only four respondents pointed out at the difficulty to understand the elements of the RMIAS (question 4):

Respondent 3: "*To some extent, if the elements are explained*."

Respondent 5: "*No, the development life cycle is too abstract*."

Respondent 12: "*It depends on the resources that the enterprise has to understand the model. For an SME, I'd suggest no.*"

Respondent 26: "*No! But then it is a complex area.*"

Answering question 5, seventeen interviewees agreed that the interrelationships between the dimensions of the RMIAS are simple. Seven respondents did not see the interrelationships as simple and provided the following comments:

Respondent 2: "*The top arrow refers to a category of information. It is not clear what is meant by a category of information.*"

Respondent 3: "*To some extent, if the relationships are explained.*"

Respondent 5: "*It is not clear or intuitive in terms of the flow of the model. The risk analysis, cost-effectiveness and consistency statements don't seem to connect.*"

Respondent 11: "*I believe the relationships within the elements are simple, but they do not necessarily flow between elements logically.*"

Respondent 17: "*Not quite. Seemingly yes, but the relationship are in reality quite complex and may vary depending on the context.*"

Respondent 19: "*Not seen as simple because the relationships could carry different meanings to different people.*"

Respondent 22: "*They are presented as such, but in reality that is not necessarily how it works.*"

Two respondents were not sure about the simplicity of the interrelationships in the RMIAS (question 5):

Respondent 4: "*They seem to be, but without applying in practice I am not sure.*"

Respondent 14: "*Not sure about the life cycle.*"

While only four interviewees did not find the element of the RMIAS simple (question 4), nine did not see the interrelationships as simple or were not sure about them (question 5). Overall, the interrelationships between the elements of the RMIAS pose more difficulties for understanding than the elements of the model. While considering the fact that a larger number of the interviewees struggled to understand the interrelationships, it is worth noting that during the presentations the author had only limited time to present the RMIAS and was not always able to provide a detailed explanation on every aspect of the model. Also the interrelationships between security concepts are complicated and may be presented in different form. They may be perceived by security experts differently. The purpose of the evaluation process was to established whether a majority of experts would agree with the representation of the interrelationships suggested in the RMIAS.

The responses for questions 4 and 5 indicate that the majority of the interviewees found the RMIAS, both the elements and the interrelationships, simple. However, in the future further research is required into the improvement of the clarity of the visual appearance of the RMIAS.

4.2.2 Accuracy of the RMIAS

In Section 4.5, where the RMIAS is compared with its predecessors, it is demonstrated that the RMIAS is more accurate than other analysed models, since it includes a more detailed taxonomy of information and classification of security countermeasures, and embraces the broader set of security goals. The RMIAS also contributes to accuracy by underscoring the distinction between security goals and security countermeasures, and by outlining the interrelationships between the concepts of IAS.

In the interviews, two questions were intended to capture the opinion of the respondents with regard to the accuracy of the RMIAS:

- Question 6 - Are the classifications included in the model accurate (the information taxonomy, the set of security goals and the types of security countermeasures)?
- Question 7 - Are the interrelationships between the elements of the model accurately described?

Answering question 6, eighteen out of twenty-six respondents agreed that the information taxonomy, the set of security goals and the classification of security countermeasures are accurate.

Three respondents (respondents 4,5 and 19) were not confident and preferred not to answer this question. Four respondents found other dimensions as accurate, but did not feel that the information taxonomy is accurate and suggested to extend it:

Respondent 1: " *The classifications encompass everything. All security goals are covered. The only thing that I would suggest is, in addition to sensitivity in the information taxonomy, take into account the purpose of use.*"

Respondent 2: "*The list of security goals is comprehensive. I have a concern about the forms of information. There may be some additional leafs in this branch.*"

Respondent 25: "*Yes, but I am not so happy with the taxonomy part though. This part is, in my opinion, relatively weak.*"

Respondent 26: "*Seem adequate, but I wonder whether responsibility should also be included in the information taxonomy area.*"

One respondent although agreed with the accuracy of other classifications, expressed a concern about the set of security goals:

Respondent 23: "*...the nuance differences between some of the security goals and the standard trio of confidentiality, availability and integrity are sometimes hard to see, e.g. trustworthiness and integrity.*"

The active discussions regarding security goals, which took place at every presentation and workshop, highlight the importance of security goals in the IAS domain. Drawing on the number of

questions regarding security goals, the author expected to receive more critical feedback with regard to the IAS-octave. Despite the expectations, the analysis of the responses shows that only one respondent expressed concern about the overlap of goals (as quoted above).

The interrelationships between the dimensions in the RMIAS were perceived as accurate by fourteen respondents (question 7). Tree respondents (respondents 4,13 and 19) were not sure about their answers. Nine respondents perceived the interrelationships as inaccurate and provided the following comments:

Respondent 2: "*The link between the first and the second dimensions is not clear.*"

Respondent 5: "*No, it requires a supporting narrative. Looks like four models which can be linked.*"

Respondent 8: "*The top left quadrant's relationships with the adjacent quadrants was not overly clear to me.*"

Respondent 16: "*Not quite.*"

Respondent 17: "*Accurate, but incomplete as the relationships between the components of the different domains of the model are not visualised in detail.*"

Respondent 20: "*No. This is where I think the problem is. A lot of it may be related to how we view the organisation and how we place the IAS in it.*"

Respondent 21: "*No, as mentioned above I don't think the interrelationship between the taxonomy and security goals quarters is accurate. I also think that in practice some analysis of the risks would be needed as well as the considerations about cost-effectiveness. Even with the prioritised security goals you will still have a very large list of risks and will need to identify which ones to tackle first.*"

Respondent 22: "*We debated the issue of whether you can classify a document before knowing your security goals, plus the risk assessment aspect continues when selecting security mechanisms (not just cost-effectiveness), rather than at the security goals stage only.*"

Respondent 24: "*I consider that the top arrow should read "The beginning of the information system life cycle" or at least "From an early stage ..." to emphasise the importance of IAS being an integral part of the information system life cycle. The Cost-Effectiveness sub label of the Select Security Countermeasures arrow might be misinterpreted as cost-benefit. Perhaps the phrase "cost-effectiveness analysis" would be more specific.*"

Among those who did not see the interrelationships as accurately described, three respondents (respondents 2,8 and 24) had doubt or suggested a clarification for the top arrow linking the security development life cycle and information taxonomy dimensions. Three respondents (respondents 21,22 and 24) suggested the clarification for the arrows linking the security goals and security countermeasures dimensions where the roles of risk analysis and cost-effectiveness analysis shall be pointed out. Two respondents (respondents 21 and 22) highlighted the inaccuracy of the link between the information taxonomy and security goals dimensions.

The additional elements suggested by the respondents such as responsibility and the purpose of use may be added to the Information Taxonomy of the RMIAS in the future. Regarding the comment provided by the Respondent 2, the analysis of the literature does not indicate that there is currently any other form of information apart from paper, verbal and electronic. However, it does not mean that is may not appear in future. Thus, for example, until first technical devices storing and transmitting information were created there was no information in electronic form. The advances of technology in future may give rise to additional forms of information in this case the RMIAS must be extended.

To address the comment of Respondent 23 regarding the differences between some of them, the justification of the inclusion of particular security goals in to the IAS-octave and the discussion of each particular goal are placed in Section 3.6 and Appendix A.6.

4.2.3 Scope (Completeness) of the RMIAS

In this thesis, this criterion is refereed to as completeness, rather than scope. Completeness has a particular importance for the RMIAS. First, in order to convey the complexity and heterogeneity of IAS, the RMIAS must cover the full range of IAS concepts. Second, the RMIAS in the next chapters of this thesis serves as the basis for the semantics of an IAS modelling notation. The above two reasons make it critical to ensure that all key IAS concepts are covered by the model.

The greater completeness of the RMIAS is demonstrated by means of benchmarking the RMIAS against other models. Table 2.6 confirms that none of the other models incorporates all four dimensions of the RMIAS. The same table shows that none of the other models considers such attributes of information as sensitivity, location and form. Only four models [86, 84, 93, 85] address time or the ISDLC, but these models overlook other critical dimensions of IAS or types of security countermeasures. According to the same table, no other model apart from the RMIAS incorporates

the drivers behind IAS decisions. The comparison with other models evidences that the RMIAS is more complete than any of the analysed models because the RMIAS (1) outlines an extensive list of security goals which is supported by the analysis, (2) incorporates the categorisation of security countermeasures which embraces all possible types of countermeasures at the high level of abstraction, and (3) addresses the drivers underpinning IAS decisions. The completeness of the RMIAS comes from adopting the broad view on an IS as a socio-technical system and from interpreting IAS as a complex multifaceted discipline, rather than a purely technical one.

In the interview, there were two questions addressing the completeness of the RMIAS:

- Question 8 - Does the model include all elements/concepts essential for the IAS domain? If, in your opinion, there are some essential, but missing from the model elements/concepts, please, name them.
- Question 9 - Does the model include any elements that are not relevant to the IAS domain?

In question 8, eighteen out of twenty-six respondents confirmed that the RMIAS is complete. Among others the following comments were received:

Respondent 2: "*The model is complete. Its completeness comes from the security goals dimension and the combination between the security goals and the information taxonomy. Further, the completeness of the model may be proved by a comparison with the other models.*"

Respondent 17: "*It seems quite complete, but depending on the context there may be different ways to categorise matters.*"

Respondent 19: "*The coverage, based on the cited literature, seems highly covering, but it is not guaranteed.*"

Respondent 24: "*As a generic abstraction, it appears to cover the principal areas I would expect.*"

Five respondents suggested to add some elements the RMIAS:

Respondent 1: "*The collaborative aspect is missing.*"

Respondent 5: "*The model needs to address more explicitly risk analysis and user cases/scenarios.*"

Respondent 12: "*The security design stage should emphasise a human factor.*"

Respondent 22: "*The role of risk assessment while selecting security countermeasures must be highlighted.*"

Respondent 26: "*I wonder whether the definition of business goals should be more explicit; this comment arises from the consideration of ICT as a 'serving system', and the underpinning idea that it is necessary to understand the 'system served'.*"

Three respondents (4,9 and 16) were not sure about the answer in question 8.

The uncertainty regarding the completeness of the RMIAS expressed by the participants is expected. A complex domain such as IAS may be approached from various perspectives which would focus on different elements of the domain, as already discussed in Section 3.12.1. The elements, which the respondents suggested to include in the RMIAS, are already addressed by it, at least, to a certain degree. For instance, the collaborative aspect is captured via the information attribute *location*. Risk analysis is addressed by the RMIAS to the degree which is required for the purposes of this model as discussed in the previous chapter. The importance of the human-factor is explicitly outlined in the RMIAS by distinguishing a whole category of human-oriented security countermeasures. Furthermore, the need to take into account the human factor during all stages of the security development life cycle, and not only at the stage of system design, is acknowledged in the RMIAS. The comment of Respondent 26 concerns the understanding of the place and role of IAS in an organisation, rather than the structure of the IAS domain. In agreement with Respondent 26, this thesis mentions (e.g. Section 3.1) that IAS does not exists for its own sake and is only used by an organisation in order to achieve its overall goals. Echoing this, in [7] the author discusses the role of IAS as a business enabler.

In question 9, only two respondents expressed concern about the relevance of some security goals to IAS domain:

Respondent 16: "*Privacy and Auditability could be argued. (Good you have included them anyway.)*"

Respondent 21: "*I think the further subdivision of the core security goals (integrity, availability and confidentiality) may assist people in understanding what the element entail, but may not add anything as separate goals in their own right.*"

Other twenty-four respondents stated that there are no elements in the RMIAS that are not relevant to the IAS domain.

4.2.4 Systematic Power of the RMIAS

The RMIAS systematises the IAS domain by distinguishing four key dimensions and, then, elaborating each dimension in depth. The RMIAS brings together these four dimensions and explains the correlations between them.

Question 10 in the questionnaire addressed the systematic power (Section 4.1.1) of the RMIAS and was worded as follows: Does the model organise elements of the IAS domain and relationships between them in a structured, systematic way?

Answering this question, twenty-two respondents acknowledged that the RMIAS presents the IAS domain is a systematic way. The following comments were received:

Respondent 1: "*The model is very good in providing the structured approach in terms of each dimension and in terms of continuous workflow.*"

Respondent 2: "*The model has a clear structure.*"

Respondent 15: "*Yes. Also it will be a good idea if you could implement this work in a form of a catalogue and with associated input and outcome for each stage.*"

Respondent 12 was not sure about the answer. Two respondents (respondents 21 and 25) expressed some reservations regarding the systematic power of the RMIAS. Respondent 21, echoing his previous comments in question 7, expressed some reservations regarding the interrelationships and provided the following comment:

Respondent 21: "*Yes, although as mentioned above I'm not sure about the relationship between the two right hand boxes and the process between the bottom two boxes.*"

Respondent 25 while found the elements of the RMIAS being systematically organised, dis not feel the same about the interrelationships.

Only one respondent cast serious doubt on the systematic power of the RMIAS:

Respondent 26: "*I am not convinced it does. There are a number of reasons for my view, not least of which is the lack of "systemic understanding" among managers. I fear the arrows in the model will be interpreted as a time dependency, rather than a logical interdependency.*"

4.2.5 Explanatory Power of the RMIAS

As demonstrated in Sections 3.9 and 4.4.2, the RMIAS may assist with the elimination of omissions and contradictions in ISPDs. It helps to identify overlooked threats, i.e. predict possible security violations and search for required countermeasures. Due to the fact that the RMIAS is more complete and accurate than the other models it may be hypothesised that the RMIAS may explain and indicate more security issues. The following example confirms this hypothesis. If accountability and legal security countermeasures are not addressed by a model (Tables 2.6 and 2.7 confirm that none of the analysed model includes accountability, and legal and organisational security countermeasures at the same time), then the model could not assist with explaining security violations that stem out of the absence of legal measures that help to keep misusers accountable for their actions. E.g. a bank logs an unauthorised access of an employee to confidential account information of bank's customers. Then, the bank attempts to sue the employee for the information misuse. The access log (e.g. the evidence received by means of a technical security countermeasure) may be insufficient in a legal mitigation, because the prosecution of an employee also depends on the clarity of the bank policies regarding information access and on the knowledge of the employee regarding his/her access rights which may be confirmed by attended security training and by a signed information access policy (i.e. organisational, human-oriented and legal countermeasures) [150].

Question 11, which was worded as "Might the Model assist with explaining (tracing back) and predicting issues related to IAS?", was intended to capture the opinion of the respondent with regard to the explanatory power of the RMIAS.

Answering this question, ten respondents saw the RMIAS as a tool that may help to explain IAS issues. The following comments were provided among others:

Respondent 2: "*The model may be used for explanation and prediction, but it should be accompanies by more detailed explanation and examples of use.*"

Respondent 15: "*Yes. I think your model will assist in predicting issues and tracing them back thanks to the goals, which occupy the third dimension of your model.*"

Respondent 23: "*Yes, using the model you would be able to trace back logically and demonstrate how an element of InfoSec had been missed.*"

Three respondents (respondents 13,22 and 25) answered in the negative to question 11. Six re-

spondents (respondents 4,5,11,16,20 and 24) were not sure about the ability of the RMIAS with helping to predict/trace back security issues.

Seven respondents found that the RMIAS may explain IAS issues, but only with some reservations:

Respondent 1: "*Due to the changing nature of a collaborative environment it is very difficult to predict something regarding security. Security audit based on the model may give some level of traceability. The model could be used retrospectively, to trace back security incidents, to see where things went wrong. But to predict will be very difficult. The model may be used for security improvements as overall process, and to certain extent for auditing and monitoring the environment.*"

Respondent 3: "*Yes, to some extent.*"

Respondent 6: "*Potentially. It is IS Risk Analysis mere.*"

Respondent 7: "*Yes. Prediction primarily.*"

Respondent 8: "*Possibly.*"

Respondent 21: "*I think in order to assist, there would need to be an element of probability assessment in the risk analysis stage.*"

Respondent 26: "*Possibly, if it is seen as demonstrating a logical dependency.*"

Coinciding with the comment of respondent 1 regarding difficulties to predict something about security, sixteen participants did not anticipate the RMIAS to be able to assist with predicting or tracing back security issues or had some remarks regarding it.

4.2.6 Reliability of the RMIAS

The reliability of the RMIAS is evaluated through the examination of two aspects.

First is the assurance that the RMIAS is valid for the majority of organisations irrespectively of size and domain. The RMIAS draws upon the wide range of IAS literature which synthesises the IAS practice of many organisations. Therefore, the applicability of the RMIAS to the majority of organisations is anticipated. Further, the flexibility of the RMIAS makes it widely applicable. The RMIAS outlines a template to which the details may be added and adjusted to suit a specific organisation as described in Section 3.3. During the workshops the usefulness of the RMIAS in the context of an SME was empirically tested. The usefulness of the RMIAS in the context of a

large enterprise is practically demonstrated by the case study. The outcomes of the workshops and case study are discussed in Sections 4.3.2 and 4.4.2 respectively.

Second is the assurance that the RMIAS leads to similar understanding when applied by different users. This aspect was tested via the workshops as discussed in Section 4.3.2.

Question 12 addressed the reliability of the RMIAS:

- Question 12 - In your opinion, would the model be valid for the majority of business organisations? Are there any industries or types of organisations where the model would not be applicable (explain your opinion)?

Answering question 12, sixteen respondents consider the RMIAS to be applicable to any organisation without exceptions (two respondents specifically pointed to its applicability in the military and healthcare environments):

Respondent 1: "*The model is suitable for the military environment. It may be applied to many organisations. For smaller organisations (e.g. sole-traders) it may be more difficult to adopt the model because of the time-consuming nature of this type of activity and a need for well-documented processes and policies. Larger organisations, obviously, may much easier spare time and effort on the model consideration and application. Larger organisations may use the model for accreditation purposes in order to define a security status of small organisations. The model follows and is aligned with the ISO standards it may be used to a number of scenarios.*"

Respondent 2: "*The model is applicable to any organisation which has information assets. I can see how the model may be applied in the medical environment. I cannot think of any counterexamples.*"

Respondent 4: "*I think the model would be valid for the majority of organisations, only the level/scale of data would vary, depending on the size of organisations and their domain area.*"

Respondent 15: "*I think, this model is promising and valid for many domain-independent organisations. ... In order to make it valid for the majority of business organisations, you must deliver it in a way flexible to receive and welcome changes from experts in the field to adapt it with their needs.*"

Respondent 24: "*Where a single organization is involved it might be a useful tool. The more interesting application would be in a multi-organisation joint venture/project, say Higher Education,*

Health Service and Pharmaceutical Company, to see if the methodology can produce a policy to meet all stake-holders' requirements."

In the opinion of five respondents (respondents 3, 7, 12, 22 and 26) the RMIAS had limited applicability. Respondent 3 had concern about the applicability of some security goals within the healthcare domain. Respondent 7 considers the RMIAS to be "*more suitable for smaller businesses with less resources*", while Respondent 12, on the contrary, stated that the RMIAS is not applicable to SMEs. Respondent 22 stated that it may be hard for large scale organisations to use the model. Respondent 26 did not perceive the RMIAS as a tool that could assist a cloud provider with defining contractual requirements.

The remaining five respondents (respondents 5, 13, 14, 19 and 20) were not sure about the applicability of the RMIAS to organisations of different types and sizes.

4.2.7 Validity of the RMIAS

The RMIAS provides guidance for the development of an ISPD (Section 3.9). Thus, the validity of the RMIAS is tested by evaluating whether the RMIAS facilitates the development of an ISPD via the workshops and case study as considered in Sections 4.3.2 and 4.4.2.

Question 13 in the questionnaire captured the opinion of the respondents with regard to the validity of the RMIAS. The question was formulated as follows: "Would the methodology embodied into the model lead to valid results (e.g. comprehensive security policies, correct prediction of InfoSec issues, meaningful tracing back of security breaches)?"

Eleven respondents (respondents 1, 2, 3, 6, 7, 8, 11, 13, 14, 17 and 19) confirmed the ability of the RMIAS to produce valid results. Eight respondents (respondents 5, 8, 10, 15, 16, 18, 20 and 24) were not able, based on the provided information, to judge the ability of the RMIAS to render valid results.

Respondents 22 and 25 answered in the negative to question 13:

Respondent 22: "*To use it to plan going forward no. I don't think so because of the lack of risk assessment incorporated into the application of the model in practice. A policy is more than the list of finalised security goals.*"

Respondent 25: "*I do not think that comprehensive security policies can be deducted from the model. I also do not think that it can predict issues since it does not consist of any instructions*

concerning the actual implementation on a managerial level. Of course, if people oversee a complete dimension then there is an issue."

Five respondents (respondents 4, 12, 21, 23 and 26) had some reservations regarding the possibility to render valid comprehensive security policies using the methodology suggested in the RMIAS. The following comments were provided:

Respondent 4: "*I think it depends on who is using/implementing the model. The level of detail plus results will depend on the knowledge of the person/people applying it.*"

Respondent 12: "*Depends on the training and understanding of the practitioner.*"

Respondent 21: "*I think to get an organisation to buy into tackling information security there would need to be some realistic risk analysis and probability assessment.*"

Respondent 23: "*Yes. However the process as attempted within the workshop seemed resource intensive prompting you to consider 5 states for each form of information e.g. account registration emails the sensitivity of that information and the location. Each of these then has 8 security goals to be assessed for applicability. This leads to an exhaustive process generating a considerable amount of data. Whilst this approach would cover every possible angle it would not seem an efficient use of resources.*"

Respondent 26: "*I can see how it would inform practitioners of particular methodologies, and that may be good enough. However, I believe that the fashion in IT is to minimise the need to "think" and the model requires users* to think *(probably, based on substantial knowledge and experience); anything that requires thinking implies, to my mind, that a range of answers may be derived. Perhaps your question should have asked whether the model can lead to "defensible" (rather than valid) results, in which case I would have offered the answer of a tentative "yes".*"

Addressing the comment of Respondent 23, it must be acknowledged that the used of the RMIAS may potentially produce an extensive list of security statement. However, it must be noted that the purpose of the RMIAS is to helps to identify a complete list of situations or scenarios where information may need protection. This inevitably will lead to a large amount of information that must be processed. It may be considered in future, however, how the development of a security policy document using the RMIAS may be simplified and optimised, but it is worth noting here that it may only be done at the expense of the completeness of a security policy document. Also the amount of data generated using the RMIAS will depend on the size of an organisation and the complexity of business. It is assumed that the larger organisations and organisations for whom

the protection of information is more critical have more resources available to assist with the generation of security policy and must allocated them more readily.

The uncertainty of a large number of respondents regarding the questioned ability of the RMIAS may be explained by the insufficient amount of information they had to make a judgement about it. The intention of the interviews was to capture int initial judgement of the experts regarding the validity of the RMIAS. It was not feasible to present to all experts interview the examples of the use of the RMIAS in several case studies. In order ro further test the validity of the RMIAS, the workshops and case study were undertaken where the participants has a chance to actually use the RMIAS.

4.2.8 Fruitfulness of the RMIAS

Fruitfulness is a desirable characteristics of a conceptual model to suggest research problems and hypothesis to be verified [27, 33].

The RMIAS, in conjunction with the examination of the literature, may assist in a search for research problems. It is described below how it may be done. Using the information taxonomy of the RMIAS, the category of information is identified. A security goal is specified for this category. The RMIAS suggests to search for a security countermeasure that may help to ensure the goal for the category of information. If the literature review shows that such countermeasure is not present (or the existing countermeasure is not efficient), then the need for a new countermeasure is detected.

The RMIAS also points to a need to explore whether there are methods to address security goals, countermeasures, and the information taxonomy at different stages of the security development life cycle. For example, the following research question was formulated in this thesis: *Is there a modelling technique that helps to address in business process models, which are designed at the stage of security requirements engineering of the security development life cycle dimension, the concepts of other three dimensions of the RMIAS (i.e. the information taxonomy, security goals and security countermeasures dimensions)?* The literature analysis which is contained in the next chapter confirmed that such modelling technique is missing. This prompted the development of Secure*BPMN which is introduced further in this thesis.

The RMIAS also provides a framework for organising/structuring research methods and findings. For example, Secure*BPMN is positioned at the stage of security requirements engineering where

it attempts to cover in full other three dimensions of the RMIAS to enable the design of a secure IS. As discussed below the majority of the interviewed academics were able to pinpoint the place of their research in the overall picture of the IAS domain using the RMIAS.

Two questions in the interviews were aimed at the evaluation of the fruitfulness of the RMIAS:

- Question 14 - Does the model provide a convenient structure for framing the existing research? How would you position your area of research/practice using the model?
- Question 15 - Could the model assist with pointing out the gaps in the existing research/practice?

Only eight respondents (respondents 1, 2, 3, 15, 16, 19, 20 and 26) had background in research sufficient to enable them to answer these questions. In question 14, while two respondents (respondents 19 and 20) were not sure about the answer, six agreed that the RMIAS provides a convenient structure for framing research. The following comments were gathered:

Respondent 1: "*Certainly, the model could help with framing the research as an overlay of the dimensions. My research is at the overlay of (1) confidentiality and technical security mechanisms and (2) availability and organisational mechanisms (e.g. processes).*"

Respondent 2: "*I can easily map my research onto the model. I would say that my research concentrates on how privacy could be achieved by technical security countermeasures.*"

Respondent 3: "*Definitely, yes.*"

Respondent 15: "*Yes it does. My research work aims to align business process architectures with business goals, which they might be hard and soft goals...*"

Respondent 16: "*The model provides a useful structure particularly with respect to encouraging users to consider forms and states of information. The subdivision of security countermeasures looks useful.*"

Respondent 26: "*.I think it could help assess competing requirements methodologies (i.e. do stories, or SSM, or personas allow effective use of the model). It has some value as a check-list for consultancy practice.*"

In question 15, where seven out of eight respondents agreed that the RMIAS may point out at the gaps in research and only one respondent (respondent 20) was not sure about the answer, the following comments were received:

Respondent 1: "*The model could certainly point out the gaps. The location parameter is particularly interesting in the cloud environment. It is interesting to see how location of information is covered from the legal and organisational side.*"

Respondent 2: "*The model could give a hint, if it is used in addition to the literature survey.*"

Respondent 3: "*Yes.*"

Respondent 15: "*Yes, definitely. Thanks again to the goals that motivate the derivation of other stages. Therefore, by using your model you may be able to detect unrequited and/or missing business-oriented objects in an organisation.*"

Respondent 16: "*Yes, due to the way the model splits out the different dimensions.*"

Respondent 19: "*Yes, I believe so. This is due to the way the model splits out the different dimensions of InfoSec and further splits these down prompting thought on each individual aspect of information security. The model starts a useful dialogue about the limitations of the CIA-triad.*"

Respondent 26: "*The model could usefully indicate a need for more knowledge. For example, given the need to consider cost-effectiveness in selecting technology, do we know what the value of, say, cryptography is? The model could be considered as defining a research agenda.*"

According to the results of the interviews, the RMIAS demonstrated fruitfulness, i.e. the ability to point out the gaps in the existing research/practice and suggest research problems. In the context of this project this quality of the model is not critical. However, it was deemed inefficient to exclude fruitfulness from the evaluation. Randomly excluding criteria from the evaluation would hinder the comprehensiveness of the evaluation of the RMIAS. The fruitfulness of the RMIAS, while not in this project, may be used by researchers in the future.

4.3 Workshops

4.3.1 Arrangement of the Workshops

Three evaluation workshops were conducted as specified in Table 4.1.

The first workshop was with the group of MSc students specialising in Information Security & Privacy at the the School of Computer Science & Informatics, Cardiff University. The group consisted of students who came straight after receiving BSc degree and did not have any practical

experience. This group was a suitable audience for testing the simplicity, explanatory and systematic powers of the RMIAS with the audience lacking the extensive experience in the IAS domain. However, the group was familiar with the ISO/IEC 27000 series of standards and, prior to the workshop, developed a security policy document for another case study using ISO/IEC 27001 and ISO/IEC 27002 standards as guidance.

The second workshops was with the group of MSc students specialising in Cyber Defence and Information Assurance at Cranfield University. This group among 13 participants included 10 mature students with experience in the IAS domain varying from 1 to 20 years. MSc students, who had practical experience in the IAS domain, were interviewed and their responses were analysed along with the responses of other IAS experts (Table 4.1).

The third workshop was with the group of IAS professionals which included an IT security expert, a personal records manager, the head and the manager of an InfoSec program.

Each group was given a one-hour presentation of the RMIAS, which, after a short break, was followed by a one-hour workshop where the participants applied the RMIAS to a case study. With the third group, both the presentation and workshop took longer as the audience was very active and many questions were asked and discussed.

During the workshops, the case study of Translate, the SME with which the reader is already familiar, was used. The case study and the task as they were given to the participants are presented in Appendix A.5. The case study outlines the current security arrangements of Translate, problems the company has been facing and the changes the business has recently undergone along with the details of the information classification scheme of the company.

Following the presentation of the RMIAS, the participants of the workshops were suggested, while working in a team of 2-4 people, to develop an Information Security Policy Document (ISPD) for Translate using the RMIAS. During two workshops, 6 teams were formed. The participants were allowed to refer to ISO/IEC 27001 and ISO/IEC 27002 standards.

It took the teams 20 to 25 minutes to get familiar with the case study. Over the remaining time each team worked on the development of security policy statements. At the end of each workshop, the participants provided their feedback on the experience of using the RMIAS.

All teams preferred to use a tabular format for the development of a policy document as suggested in Section 3.9. First, the teams produced tables in MS Excel (or another spreadsheet application) which they populated with the combinations of four information attributes and security goals as

described in Section 3.9. Then, the groups discussed each combination. They attempted to work out a scenario corresponding to each combination and make a judgement on whether a scenario posses any threats to Translate. If they answered positively on the last question then the teams identified security countermeasures that may help to achieve the security goal for the category of information under consideration.

The length of the workshops did not allow the participants to develop a complete or extensive ISPD. The number of statements each team managed to produce during a workshop vary from 3 to 8. Since the RMIAS only provides a template to be filled in with policies, the quality of policy statements strongly depends on the knowledge and experience of its developer(s) and on information they have at hand. Therefore, the quality of security policy statements does not adequately reflects the merits of the RMIAS and was not explicitly assessed. However, the viability and compliance to reality of the security statements developed by the teams were assessed by the author and, then, confirmed with one other IAS expert, who has experience both in academia and industry and who was present at the workshops. The ISPD statements developed by the participants of the workshops may be found in Appendix A.9.

Since it was not feasible to evaluate the completeness and quality of the ISPDs developed by the participants, the purpose of the workshops was to observe how well the RMIAS is comprehended by the participants with the different levels of expertise in IAS and whether the participants are able to use the RMIAS while working in a team, and to gather the feedback of the participants on the use of the RMIAS. The collected information is analysed in Section 4.3.2.

4.3.2 Feedback from the Workshops

The workshops confirmed that the majority of the participants managed to get a solid understanding of the RMIAS and how a policy document may be developed using the RMIAS. There was only one team of three MSc students who significantly struggled with the task. However, after additional help the team managed to produce 3 valid policy statements. Other teams worked independently and only in several cases called for minor clarifications.

The final feedback of the participants indicates that the participants appreciate that the RMIAS helps with profiling information - "*the complete registry of all information organisation has is good because nothing is omitted from a policy document*". Each team was able to identify the scenario in which a specific category of information needed protection from threats refereed to by

a specific security goal.

The IAS-octave was found by the participants useful. According to the feedback of the teams "*the IAS-octave covers all possible issues with information*". The participants also appreciated the help the RMIAS provides with the identification of scenarios in which information needs protection.

There was only one MSc student who struggled with the concept of security goal. The student suggested to include in the final table, along with the name of a security goal, more detailed description of attacks and threats to which the goal refers to. This approach is not optimal as discussed in Chapter 2, as it leads to the duplication of information. However, it is suggested when presenting the RMIAS in future and, the IAS-octave specifically, to provide an audience with more examples of threats and attacks which pose threats to each security goal.

According to the comments of the participants of the workshops, using the RMIAS it was easier to see how an ISPD must change (i.e. which security statements to be included, excluded or corrected) when a change in an organisation which affected any of the elements of the RMIAS took place. The participants also suggested that the RMIAS may serve as a tool for benchmarking of the ISPDs of different organisations which may be specifically fruitful in the context of a collaborative environment and cross-organisational information sharing. Thus, the RMIAS may help to see the differences between the document classification as well as location categorisation schemes of different organisations. It may also highlight the difference of the approaches to IAS by comparing security goals (and their definitions) and the types of security countermeasures which are recognised and exploited by different organisations. Furthermore, the RMIAS may help to compare which security countermeasures are used by different organisations in similar situations. This may be helpful when ensuring the compliance of the security policies of one organisations with the policies of another one and in certification.

The group of MSc students, who previously developed an ISPD based on the ISO/IEC 27001 and ISO/IEC 27002, was able to compare the process of the development of an ISPD guided solely by the ISO/IEC standards and the same process guided by the RMIAS in conjunction with the ISO/IEC standards. The feedback of this group indicated that the use of the RMIAS aids in judging the completeness of an ISPD. The RMIAS helps to ensure that all possible problematic situations and all categories of information are covered by an ISPD, while working with the ISO/IEC standards only, there was no way to make any judgement regarding the completeness of an ISPD. One of the teams also noted the benefits of the explicit declaration of knowledge as one of the forms of information which needs protection. The team said that discussing how different security goals

may be achieved for knowledge or verbal information greatly assists with the identification of security violations scenarios and, consequently, security statements covering knowledge protection, which would unlikely emerge during the work on an ISPD otherwise.

The group of practitioners who participated in the third workshop indicated that it is always challenging to reflect all possible threat situations in an ISPD as there is no framework based on which one can gauge whether everything is addressed or not. The group agreed that the RMIAS provides useful guidance on how the complete set of such situations may be determined. The group also agreed that the IAS-octave certainly prompts one to consider more threat scenarios than, for example, the CIA-triad. Although this group originally voiced a concern about the overlap between some security goals (as addressed in Chapter 3), after working on the Translate case study the group agreed that the explicit acknowledgement of all eight goals of the IAS-octave was helpful, specifically, for the audience inexperienced in IAS. If any of the goals was omitted from the model, then an organisation relies purely on the knowledge and expertise of an expert developing an ISPD to identify and address threats to information which the omitted goal covers.

The group of participants from Cranfield University also suggested that the RMIAS may serve as a tool for security audit and benchmarking by large and small organisations. The participant, who had experience in the field of IAS consultancy also predicted that the RMIAS may serve as a consultancy framework.

4.4 Case Study

4.4.1 Arrangement of the Case Study

This is a case study of an executive non-departmental public body based in the UK. The name of the organisation may not be revealed due to the non-disclosure agreement. Further in the text, the organisation is referred to as the Agency. The Agency has multiple offices across the UK and employs over 1000 people.

The Agency provided the author with four ISPDs:

1. Agency data security standard (8 pages);
2. Classifying and handling sensitive information policy (25 pages);

3. Sending, transferring and storing data policy (3 pages); and

4. Protective security policy (3 pages).

The provided documents were initially analysed to identify which elements of the RMIAS are present. The examination of documents confirmed that all elements of the RMIAS were present in the policies. The precise values of the elements were extracted and are stated below.

The organisation uses the UK government sensitivity classification and marking scheme: Top Secret, Secret, Confidential, Restricted, Protect and Unclassified [109][5].

The following locations are listed in the examined policy documents: the Agency offices; the supporting IT company; the third parties storing information on behalf of the Agency; home environment (employees who work from home); and locations other than the above. It was agreed to categorise the locations as suggested in Section 3.5.3: *controlled* - the Agency offices, *partially controlled* - the supporting IT company and third parties storing information on behalf of the Agency and home environment (employees who work from home); and *uncontrolled* - locations other than the above .

The state of information is acknowledged in the analysed documents. It was specifically noted that countermeasures were specified for the protection of information at the stages of creating and destruction as well as at the stages of processing, transmission and storage. This further confirmed the correctness of the incorporation of these stages into the information taxonomy of the RMIAS.

Security countermeasures of all four types, namely legal, technical, organisational and human-oriented were encountered in the analysed policies. As it was anticipated, the analysed documents stated only the CIA-triad (confidentiality, integrity and availability) as the security goals to be addressed.

After all elements of the RMIAS were identified, the RMIAS was adjusted with the values specific to the Agency (e.g. information sensitivity and location classification) as depicted in Figure 4.2. The IAS-octave replaced the CIA-triad and was used in the analysis.

[5]The government classification scheme was changed in 2013 [110] after this case study was performed.

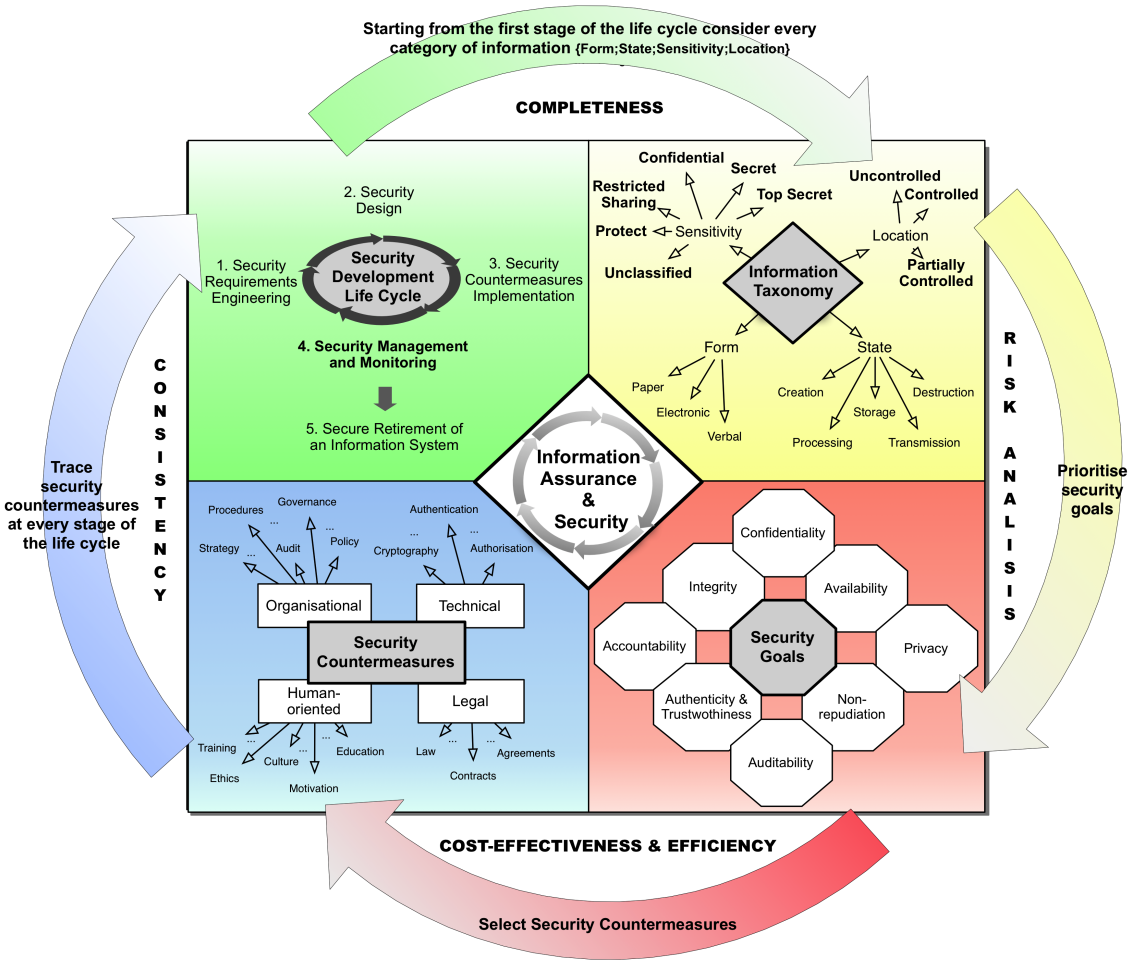


Figure 4.2: The RMIAS as adjusted for the Agency

Using the values of information sensitivity and location specific to the Agency, a table was created as described in Section 3.9. The table was populated with all possible combinations of the values of such parameters as information form, information sensitivity, information location, information state and security goal. The table was created and populated using Microsoft SQL Server 2008. The work was done from the MS SQL Management Studio environment directly and no user interface was developed.

Then each security statement in the analysed documents was examined and assigned in to the appropriate combination of the information category and security goal (i.e. the column Security Countermeasure of the table in a specific row in the table was populated with the description of this security countermeasure).

For example, when the statement "Documents marked *Confidential* may be taken home only with a written approval of a designated person" was examined it was assigned to the row with the

Table 4.2: The structuring of an Information Security Policy Document using the RMIAS (excerpt).

	1. Form	**2. Sensitivity**	**3. Location**	**4. State**	**5. Security Goal**	**6. Security Countermeasure Type: Policy Statement**
1	Paper	Secret	Controlled	Creation	Confidentiality	Organisational: *Apply Protective Marking (Avoid over or under marking*).
2	Any	Any	Controlled	Destruction	Availability	Organisational: *No information, held on any media, can be destroyed unless it has been reviewed.*
3	Paper	Confidential	Partially Controlled	Transmission	Accountability, Confidentiality	Organisational: *Documents marked CONFIDENTIAL may be taken home only with a written approval of a designated person. All actions with documents marked CONFIDENTIAL to be logged.*
4	Electronic	Protect	Uncontrolled	Storage, Processing	Confidentiality, Integrity	Technical: *Any data marked PROTECT must be encrypted when taken outside the office*.

following characteristics: information form - paper, sensitivity - *Confidential*, location - partially controlled, state - transmission, security goal - confidentiality.

The complete version of the final table, which was created after all four documents were examined, may not be presented in the thesis due to the non-disclosure agreement. However, the excerpt from the final table is shown in Table 4.2. It is sufficient in order to understand how the policy documents were structured. The security policy statements outlined in the last column of Table 4.2 are retrieved from the ISPDs of the Agency.

For example, row 1 refers to the paper documents which are created in the organisation's office and classified as *Secret*. In order to achieve the confidentiality of information classified as *Secret*, at the stage of creation protective marking must be applied to the information. Row 2 refers to documents in any form and of any sensitivity which are destroyed in the office. The policy outlines an organisation countermeasure which is required to protect availability, namely "any documents must be reviewed before they are destroyed".

In the table, if several countermeasures were relevant to the same combination of information

category and security goal, all countermeasures were placed in the last column of the appropriate row.

In the final table the rows were flagged which contained the combinations of information categories and security goals for which no security controls were specified in the analysed documents (i.e. the last column of the final table was empty for the row). These rows refer to the situations which were not addressed by the analysed polices.

The final table was presented to and discussed with the Information Security Officer of the Agency. Two meetings took place. At the first meeting the RMIAS was presented and initial information was received from the Agency. The exchange of email helped to identify the missing information. At the second meeting the finalised table was presented to the Agency, and feedback was received. Both meetings were run informally and comments were provided in a free form. These comments are discussed in Section 4.4.2.

4.4.2 Feedback from the Case Study

While in the workshops the RMIAS was exploited to produce an ISPD from scratch, in this case study the RMIAS was employed to structure and organise the existing ISPDs.

The Agency willingly adopted the RMIAS because it had no other model of IAS in place. According to the Agency, the RMIAS "*makes perfect sense*" in the context of the Agency and provides a way of approaching security in a more structured way.

At the first meeting, the Agency saw the IAS-octave as the main advantage of the RMIAS. Since the existing policies of the Agency were confined to the CIA-triad, the Agency anticipated that considering the wider spectrum of threats beyond the CIA-triad may help to improve the policy documents and address the threats that were potentially overlooked. The Agency also positively evaluated the segregation of legal security countermeasures. A discussion took place on whether it is legitimate to consider law as a security countermeasure and the agreement was reached that it is, since an organisation may refer to law in order to protect its information.

At the second meeting, it was agreed by the Agency that the information taxonomy and security goals dimensions of the RMIAS provide a basis for a good coverage of all potential situations in which information needs protection ("misuse cases"). It was confirmed that by using the RMIAS, more potentially dangerous cases where information needs protection may be identified.

The policy statements of the Agency were spread over a number of documents developed and updated by a number of employees at different time. Therefore, the fact that the RMIAS helps to organise the policies extracted from various policy documents in a form which is easy to manage and analyse, was seen as one of the major positive outcomes of the use of the RMIAS.

The final table of the Agency's security policies, which is discussed and the excerpt from which is contained in Table 4.2, enabled the Agency to see the range of the countermeasures of different types declared in various documents and applicable to the same category of information for achieving the same security goal. This provided a basis for a cost-effectiveness and efficiency analysis, and for the improvements of the ISPDs (i.e. duplicated countermeasures may be removed or the most cost-effective alternative may be chosen).

The Agency expressed interest in a software system which will be based on the RMIAS and will provide security recommendations for particular situations and particular categories of documents. The decision-making support system based on the RMIAS is further discussed in Section 8.2, where the future work that stem from this thesis is outlined.

The case study confirmed that the RMIAS (1) helps to organise, in a manageable form, security policies spread over multiple documents, (2) permits the tracing of the contradictory security policy statements, and, most importantly, (3) facilitates the identification of omissions in security policies.

4.5 Comparison with Other Models

The analytical evaluation is continued in this section. It is discussed below how the RMIAS addresses the drawbacks of the existing IAS models which are enumerated in Section 2.9, and the recent trends in the IAS domain, which are outlined in Section 2.4:

- *The model development method and the analysed sources of information are not discussed.*

  The RMIAS development method is in detail outlined in Section 3.1 along with the range of the literature analysed. The RMIAS was developed following the scientific method such as the Best-Evidence Synthesis approach [97]. In the RMIAS the reasons for the inclusion of each dimension are explained. The aspects of IAS, which are not (or, at least, not explicitly) included in the RMIAS, are also discussed (Section 3.11) and the vindication of non-inclusion is given.

Table 2.5 indicates that comparing with the other models of IAS, a more extensive set of information sources was analysed while developing the RMIAS. The systematic literature review method, which was exploited for the selection of the existing models and frameworks of IAS to be included in the analysis, is described in Section 2.8.1. The range of the literature examined in order to build the RMIAS extends far beyond the existing models of the IAS domain. The examined sources related to IAS in general and to each aspect of the RMIAS are referenced in Chapter 2 and in the current chapter respectively.

The explicit development methodology of the RMIAS helps to corroborate the validity of the model.

- *The classification of security countermeasures, if encountered, does not cover all possible countermeasures*.

  The RMIAS suggests a categorisation of security countermeasures which distinguishes four types of security countermeasures (technical, organisational, human-oriented and legal). Table 2.6 shows that only one other model [87] apart form the RMIAS incorporates all four types of security countermeasures. However, the model in [87] does not include such critical IAS concepts as a security goal and the security development life cycle. Only the model in [89] brings to attention the importance of the ethics and morals of IAS specialists. This aspect is overlooked in other models, but is crucial since ethical issues often emerge in IAS (e.g. financial evaluation of risks to human lives [151] and privacy). The RMIAS incorporates ethics into the category of human-oriented security countermeasures along with motivation, morals and the like. By referencing the broad range of diverse by nature security countermeasure, via the security countermeasures dimension the RMIAS conveys the multi-disciplinary nature of the IAS domain and the fact that IAS is not confined to the technical security solutions. Thus, the RMIAS promotes an holistic approach to IAS.

- *A model does not provide an alternative for the CIA-triad or a proposed alternative is not justified.*

  The RMIAS incorporates the IAS-octave. The IAS-octave development method is in detail described in Section 3.1. The extensive range of the IAS literature was analysed to support the IAS-octave. The detailed discussion of the meaning of each goal is given in Section 3.6, explaining the origins of the adopted approach to each security goal. The applicability of security goals to the components of an IS is clarified. During the development of the RMIAS, the IAS-octave was multiple times discussed with the IAS practitioners and aca-

demics. The literature analysis which supports the development of the IAS-octave along with the transparent development method corroborate to some degree plausibility of the IAS-octave. The completeness and validity of the IAS-octave are further tested as a part of the RMIAS evaluation processes as described in this chapter.

- *A model does not addresses the realities of cross-organisational information sharing.*

  To address the protection of information outside the organisation's perimeter, the RMIAS incorporates into the Information Taxonomy dimension such attributes of information as location and sensitivity. In the IAS-octave, such security goals as non-repudiation, authenticity & trustworthiness, and accountability also refer to the interactions of an organisation with external parties. Thus, the RMIAS considers an IS not as a "closed" system, but takes into account the influences of the external world on an IS.

- *The notion of time within a model has no practical value.*

  The RMIAS incorporates the Security Development Life Cycle as one of its dimensions, highlighting the need to address IAS consistently at all stage of the ISDLC.

- *The visual appearance of a model is not explained or justified.*

  The visual appearance of the RMIAS is discussed in Section 3.10 where all design decisions are explained. The transparency of the design decisions improves the comprehension of the model and makes the analysis of its cognitive effectiveness, which may be undertaken in future, easier. This is further mentioned in Section 8.2, where future work is discussed.

- *No analytical or empirical evaluation of a model is carried out.*

  As highlighted in Section 2.9, one of the drawbacks of the analysed models of IAS is the lack of evaluation. More specifically, none of the analysed models are evaluated with the involvement of people other than the model developer(s) (Table 2.5). This drawback of the existing models is fully addressed in the RMIAS. As this chapter describes, during this research project, the RMIAS was thoroughly evaluated both analytically and empirically with the involvement of other people.

4.6 Discussion

This section discusses the evaluation results and, at the end, outlines the limitations of the carried out evaluation.

In the discussions of IAS with a large number of experts specialising in different areas of IAS and with a number of people lacking an extensive experience in IAS, a coherent understanding of the IAS domain and the use of an agreed-upon terminology proved in practice to be critical for the effective communication with regard to IAS. This provided a further confirmation of the importance of this part of the research project.

During the presentations and workshops, the participants demonstrated genuine interest in the RMIAS. They were actively involved in the discussions of the model and willingly provided constructive feedback on the model. In fact, all individuals with whom the RMIAS was debated during the development and evaluation process were sincerely interested in the model and often mentioned how they might make use of the RMIAS in their research or practice. In the author's opinion, the above corroborates, first, the importance of the representation of the knowledge of the IAS domain and, second, the ease of the comprehension of the RMIAS. The latter conclusion draws upon the believe that people get more actively involved in the debates on the subjects which they understand.

The results of the interviews are summarised in Figure 4.3 (the supporting table with the results is presented in Appendix A.13). The y-axis shows the questions in the interviews and the evaluation criteria they correspond with, and the x-axis shows the number of the responses. Regarding each of eight criteria, more than a half of the respondents agreed that the RMIAS satisfies the criterion. However, the accuracy of the interrelationships between the dimensions of the RMIAS received the lowest support (14 respondents). The relevance of the elements of the RMIAS received the highest support (24 respondents). The simplicity and accuracy of the elements was supported by 22 and 18 respondents respectively. The completeness of the RMIAS was endorsed by 18 respondents.

The participants of the workshops, even those who had limited experience in IAS, were able to exploit the RMIAS for the development of an ISPD after only a one-hour presentation of the model. This also supports the hypothesis that the RMIAS represents the essence of the IAS domain at a level which is easy to comprehend even by a novice audience. As was noted by the participants of the workshops, the RMIAS is a more effective way of describing IAS than as a set of definitions or rules. Many participants stated that with the RMIAS they acquired a more comprehensive vision of IAS (some even described it as "*eye-opening*"). Many participants were able to pinpoint the place of their personal topic of interest in IAS in the overall picture of the domain.

During the presentations and workshops, the IAS-octave usually sparked intensive discussions. The participants challenged the meaning of and the differences between security goals. In these

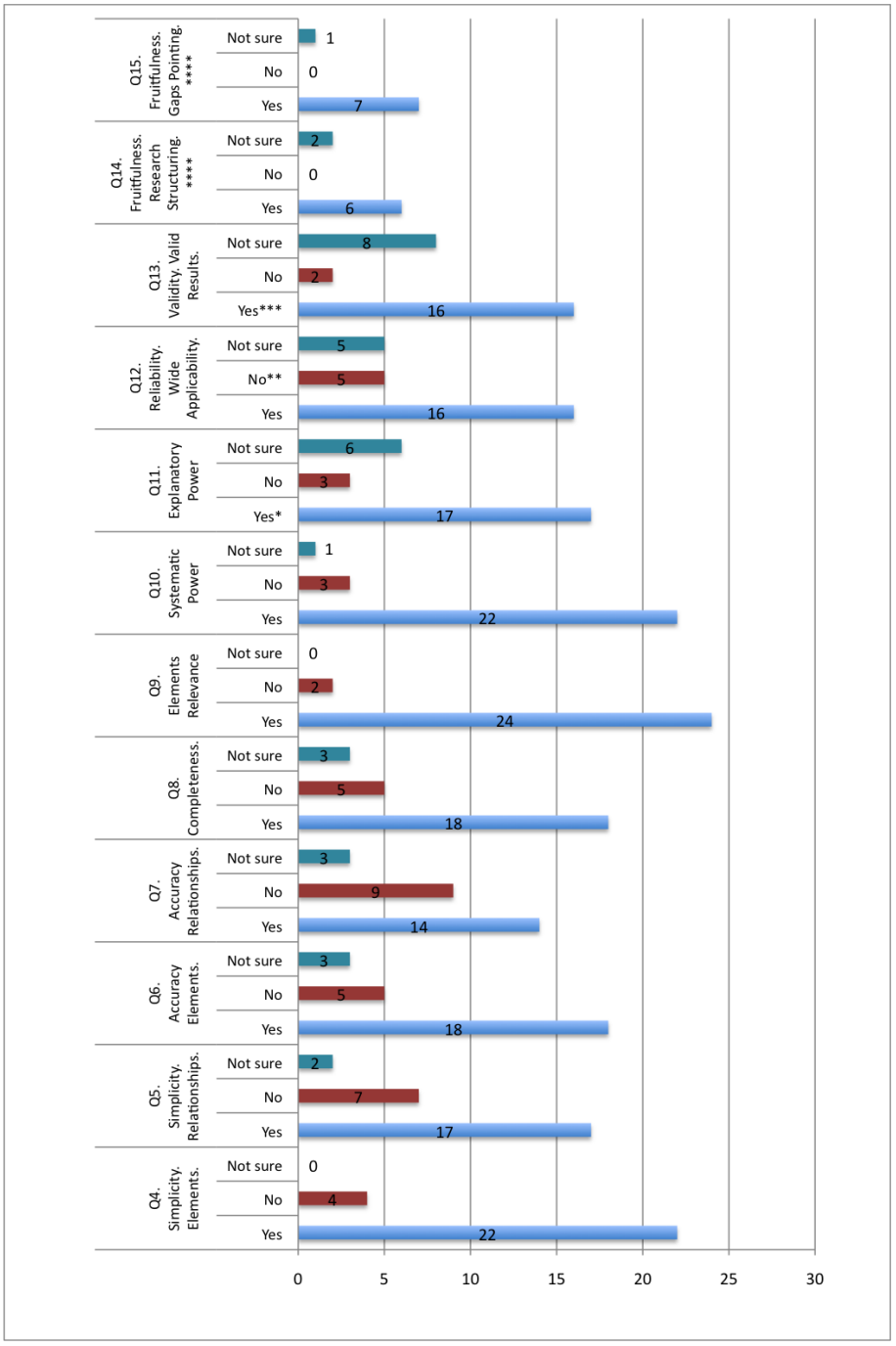


Figure 4.3: Summary of the Interview Answers

Notes:

* - includes 10 respondents who answered "Yes" and 7 respondents who answered "Yes, with some reservations";

** - refers to the participants who pointed out at the limited applicability of the RMIAS;

*** - includes 11 respondents who answered "Yes" and 5 respondents who answered "Yes, with some reservations";

**** - only 8 participants were invited to answer this question.

discussions, the IAS-octave was acknowledged to be more comprehensive than other sets of goals (e.g. the CIA-triad) and to cover all known to the participants threats to information. From twenty-six experts interviewed, only two were concerned about the relevance of two security goals (Section 4.2.3). No additional security goals were suggested during the interviews or workshops. These results along with the IAS-octave development methodology (Section 3.1) corroborate the completeness and accuracy of the IAS-octave.

The majority of interviewees agreed that the RMIAS provides a complete and accurate representation of the IAS domain (Figure 4.3). In agreement with the interview results, the workshops and case study also confirm that the RMIAS is complete and accurate at the level of abstraction required to facilitate the discussion of IAS with the purpose of the development of an ISPD.

The evaluation results endorse the reliability of the RMIAS in two ways. First, the results of the interviews corroborate the applicability of the RMIAS for the majority of organisations. The experts anticipate no or little restrictions to the fitness of the RMIAS in the context of any specific domain (Section 4.2.6 - question 12; Figure 4.3). Furthermore, the case study demonstrated how a large-scale organisation may avail of the RMIAS, while in the workshops the RMIAS was successfully applied in the context of an SME (Sections 4.3.2 and 4.4.2). Second, the workshops, demonstrated that the RMIAS leads to the congruous understanding of the IAS domain when applied by different users. The participants of the workshops were able to work as a cohort to produce security policy statements using the RMIAS.

The analytical evaluation of the RMIAS as well as the interviews with the IAS domain experts did not explicitly cover the cognitive effectiveness of the visual appearance of the RMIAS. However, during the workshop at Cranfield and Cardiff Universities, while providing the feedback on the RMIAS, the participants of the workshops explicitly highlighted the clarity and cognitive effectiveness of the RMIAS as one of the strengths of the model. This work does not make any strong claims with regard to the cognitive effectiveness of the RMIAS because it was not the primary focus of this research project. Nevertheless, it is worth pointing out that to the best of the author's knowledge, the RMIAS is the first model which provides the design rationale for its visual appearance (Section 3.10). The future work regarding the visual appearance of the RMIAS and its evaluation is further mentioned in the last chapter of the thesis.

During the evaluation, the IAS experts suggested a number of the implications of the RMIAS. The experts saw in the RMIAS a consultancy framework and a basis for an IAS decision-making support system. The future work that may stem from this is also considered in the last chapter of

the thesis

The systematic power and explanatory power of the RMIAS were confirmed by the results of the interviews and supported by the observations of the audience during the presentations and workshops. The systematic power and explanatory power of the RMIAS were acknowledged by 22 and 17 respondents respectively (Figure 4.3). The RMIAS demonstrated itself as being accessible to a novice audience as well as to the experts in the domain. The accuracy of the elements of the RMIAS and the completeness of the model, which both were endorsed by 18 respondents, and proved in the analytical analysis (Section 4.2.3 and 4.5), make the RMIAS a solid basis for the semantics of an IAS modelling notation.

The workshops and case study which tested the reliability and validity of the RMIAS demonstrated that the RMIAS (a) is applicable to large and small organisations of different domains, (b) leads to similar understanding of the IAS domain when used by different users, and (c) helps to render a valid ISPD and structure it in a useful way. The conclusion regarding acquiring a similar understanding of the domain is based on the observations that (1) during the presentations and workshops, the participants asked meaningful questions, i.e. they all understood the model in a way it was intended, (2) the participants were able to use the model while working in a team, i.e. within a team there was an agreed-upon understanding of the domain and its main concepts, and of the way how it must be applied to a specific case, and (3) all six teams of the workshops' participants developed meaningful security policy statements which all had a resemblant format, i.e. the understanding of the RMIAS and the way it must be used for the development of an ISPD for a specific case was also coherent among the teams.

There are a number of limitations to the evaluation process which are outlined below. The results of interviews may be affected by many factors [146] including the command of language and background of both interviewee and interviewer, the inconsistent interpretation of terminology, the lack of motivation, etc. To address some of the factors above, the semi-structured interviews and the "thick" reporting of the interview responses were exploited. The RMIAS provided the IAS terminology which was consistently used during the presentation, workshops, interviews and the reporting of the results. In this research project, although the participants were not financially or in any other way motivated to participate in the evaluation process, they demonstrated, as mentioned above, a profound interest in the RMIAS, and readily and actively participated in its evaluation.

It may be debated how well the MSc students, who were involved in the evaluation, stand proxy for a novice audience. Although the group at Cardiff University had no practical experience in IAS,

they already were taught several modules on IAS by the time the evaluation took place. Hence, although they knowledge was limited, they were not complete novices to IAS.

The suitability of the RMIAS for an SME was only demonstrated in the workshops with MSc students (though many students at Cranfield University had practical experience in IAS) on the case study of Translate. During this project, there was no possibility to test the RMIAS in the settings of a real SME. The author of the thesis faced difficulties with finding real life case studies. Although the companies, who the author managed to get in contact with, expressed interest in the RMIAS, they were reluctant to discuss their security issues with a PhD student. It was, therefore, a significant success of this research project to find an organisation (referred to as the Agency) who agreed to collaborate with the author and to get involved in the practical evaluation of the RMIAS.

Finally, there were a number of critical comments regarding the RMIAS received during the interviewing process. All the comments are discussed in the proceeding sections. In this thesis, the RMIAS is presented in the same form as it was presented to the experts interviewed. The RMIAS has not been modified according to the comments and this is left for future work.

4.7 Chapter Summary

In this chapter, the RMIAS is evaluated in order to achieve Objective 2.B of this thesis (Section 1.3).

The evaluation results corroborate the fact that the RMIAS is a valid way of representing the IAS domain. The majority of the experts, who were interviewed, agreed that the RMIAS reflects their understanding of the IAS domain and complies with the quality characteristics the model was assessed against. It is demonstrated, via the case study and the workshops, that the method of the ISPD development suggested in the RMIAS is viable and useful. This further confirms that the representation of the IAS domain as conveyed by the RMIAS is adequate, complete and accurate to the level of detail sufficient for the discussion of IAS issues in multi-disciplinary teams and the development of ISPDs. The evaluation confirms that the RMIAS conveys the IAS domain knowledge in a way which is suitable for an audience who has little or no experience in IAS as well as for more experienced users.

The RMIAS was the subject to peer review and scrutiny in the Security Ontology workshop, which was held in conjunction with the Eighth International Conference on Availability, Reliability and

Security (ARES) in Germany. It is published as a part of IEEE conference proceedings [96].

At the time of the thesis submission, according to Google Scholar, there are twelve independent of the author citations of the paper which introduces the RMIAS. Moreover, within the short period of time after its publication, the RMIAS was adopted by other researchers, independently of the author of the thesis, to serve as the basis for a security extension for a business process modelling language in [152] (this proposal is discussed in the next chapter in Section 5.4.2.15). The choice of the RMIAS in [152] is explained as follows: "*we choose the Reference Model on Information Assurance and Security (RMIAS), as it is the result of an analysis and classification of security aspects proposed by the most known reference models on information assurance and security. As far as our knowledge goes, it proposes the most comprehensive set of security aspects...*" [152]. It is worth noting here that in [96] the RMIAS is presented only as a novel representation of the IAS knowledge and the potential use of the RMIAS in the context of security extensions for business process modelling language is not mentioned.

Furthermore, in July 2014, the Swedish Tax Agency requested a permission to use the RMIAS in their training materials on IAS.

All the above verifies Hypothesis B, stated in Section 1.4: *The RMIAS provides more complete and accurate representation of the IAS domain, than the existing conceptual models of the IAS domain. The RMIAS reflects how the IAS domain is understood by IAS domain experts and represents the domain in the form accessible by the experts with different backgrounds and with the different levels of experience in IAS. Due to the above, the RMIAS helps to build a congruous understanding of the IAS domain in a multidisciplinary team of experts and provides a solid basis for the semantics of Secure*BPMN.*

Thus, the evaluation presented in this chapter as well as the fact that the RMIAS is rapidly gaining the acceptance of researchers proves that the RMIAS is well suited to underpin an harmonised understanding of the IAS domain in a multidisciplinary team of experts and provides a solid basis for the semantics of Secure*BPMN, the IAS modelling notation the remainder of this thesis elaborates on.

In the following chapter, the reader is introduced to business process modelling and its integration with IAS. The existing security extensions to business process modelling languages are examined and, a specific attention is paid to the bases they use for their semantics. The comparison of the RMIAS and the bases used to support the semantics of other notations is drawn. After that, in Chapter 6 the RMIAS is employed as the foundational basis for the semantics of Secure*BPMN.

Chapter 5

Examining the Integration of IAS into BPM

This chapter provides a brief introduction to the Business Process Management (BPM) domain and outlines concepts, which are required in order to appreciate the context and contribution of this thesis. While presenting the related concepts, the approach adopted in and the scope of this thesis are clarified. This chapter also outlines the literature review methodology exploited in this thesis and contains the detailed analysis of the existing security extensions for Business Process Model and Notation (BPMN). The shortages of the analysed security extensions for BPMN are debated and then summarised in the final section of the chapter.

5.1 Business Process Management and Modelling

The main assertion of BPM is that any goal and any outcome is achieved by an organisation through the performance of a number of activities.

The term BPM came to existence and gained a particular popularity at the end of the 20th century. There are various approaches to BPM. Some authors place the emphasis on the IT component and the suitability of processes for automation, while others - on the management component and on the role of business process in the improvement of business performance and efficiency [10]. According to the definition in [17], *BPM incorporates concepts, methods, and techniques which support the design, administration, configuration, enactment, and analysis of business processes*. This definition promotes the IT-focused view on BPM, by emphasising the configuration and enactment steps of BPM. From the management point of view, BPM includes all actions aimed at the analysis, coordination and improvement of fundamental activities of an organisation (e.g. manu-

facturing, marketing, communications etc.) which are performed in order to achieve business goals and to deliver value to customers [153]. In this thesis, BPM is approached mainly from the management point of view, while the automation of business processes is secondary.

In [154], the following steps of the BPM life cycle are outlined: design, system configuration, process enactment and diagnosis. According to [155], BPM consists of four main activities: modelling, automation or deployment, optimisation and management. Thus, irrespective of the adopted viewpoint of BPM, the first stage in the BPM life cycle is the modelling (or design) of business processes. This thesis focuses on the first stage of the BPM life cycle.

Business process modelling deals with the representation of a process in the form of a graphical model [156]. Business process models are taken as an input for the succeeding steps of BPM. Therefore, efficient business process modelling is indispensable for the overall success of BPM [156]. Business process models make business logic more transparent, easier to monitor and analyse, and, as a result, more agile.

Business process modelling may be performed for various purposes [9, 157, 158]:

1. Description and documentation, in order to define and communicate a process and enhance the human understanding of it;
2. Management and monitoring, in order to serve as a guidance for the human performance of activities as well as to track performance and assess compliance with requirements;
3. Analysis, in order to identify opportunities for improvements; and
4. Enactment, in order to produce an executable code.

The purpose for which business processes are modelled defines the characteristics of resulting models (e.g. the levels of detail etc). This thesis is concerned with the representation of security concerns in models developed for purposes other than enactment.

5.2 Levels of Abstraction

A business process may be specified at different levels of abstraction [17, p.17]:

- *Organisational business process models* - characterise business functionality at the coarse-grained level and outline goals, expected results, dependences on other organisations etc. These models are usually specified in a textual/tabular form and may be accompanied by ad-hoc diagrams (e.g. process landscape diagrams).

- *Operational business process models* - outline business activities and the dependencies between them. Operational models depict the logical order of activities, roles and responsibilities, and information objects [9]. Operational models are typically expressed using graphical business process modelling languages. These models are more detailed than organisational ones, but they still disregard execution details. Operational models require a lower level of formality than executable models, because "*while computers have precise execution semantics, humans do not*" [158, p.82]. Humans are able to understand business processes defined at a high level of abstraction, due to the fact that humans are flexible and are able to fill in the missing information before enacting a process [158].

- *Implemented business process models* - contain detailed technical information about a process and are developed in order to enable the implementation of a process by a software system. Implemented models may differ from operational models (e.g. in terms of the order of activities) due to the technical capabilities of software infrastructure [9]. A workflow is a type of implemented business process. While a *workflow*, a deployable version of a business process enriched with execution details, presents a realisation view, the term *business process* refers to the business logic and a conceptual view of the set of activities performed by an organisation [10].

The interest of this thesis lies in how security may be integrated into *operational business process models destined for human understanding and enhancing communication*. Operational models are more suitable for the facilitation of the discussion of security issues by a multidisciplinary team than other models. Organisational models are too abstract and do not outline enough details of a business process, while implemented business process models are, on the contrary, overloaded with execution details which distract from security-annotations. The limited complexity of operational models makes them accessible to a wide range of experts, even to those who lack the extensive knowledge of a modelling language in which the models are expressed.

The representation of security details within implemented models (workflows), which are enacted solely by software systems, is already well researched as discussed in Section 5.4. It is, therefore,

out of the scope of this thesis. In this thesis, security-annotations are developed for business processes which are not automated or are partially automated and are enacted by humans with or without the help of a software system.

Analysing the requirements for models developed for different purposes, Curtis et al. [158] state that the main requirements for models which are intended to support human understanding and communication are expressiveness, comprehensibility and communicability. Hence, not any model is suitable for enhancing communication and understanding, and, as a result, for the security-annotation suggested in this thesis. The requirements for the models suitable for Secure*BPMN-annotation are outlined in Section 7.2.2.2.4.

5.3 BPMN

5.3.1 Justification of the Choice

There are many business process modelling languages including UML activity diagram, Event-driven Process Chain (EPC), IDEF, Petri nets, Role Activity Diagram (RAD), etc.

The Business Process Model and Notation (BPMN) is a flowchart-based graphical notation designed for modelling business processes. BPMN is a de-facto industry standard in the domain of business process modelling [159]. BPMN (originally titled Business Process Modelling Notation) was developed by the Business Process Management Initiative (BPMI). Since 2005, after the merging of the BPMI and the Object Management Group, BPMN is maintained by the Object Management Group. BPMN 2.0 [160] was released by the Object Management Group in January 2011. The second version of the notation (1) standardises process execution, (2) defines a common meta-model to enable the exchange of models between BPMN compliant tools, and (3) introduces the concept of choreography. In November 2013, BPMN 2.0.1 was published as an international standard ISO/IEC 19510:2013(E) [161]. Further, in this thesis the reference is always made to BPMN version 2.0.1 as specified in ISO/IEC 19510:2013(E) [161], unless otherwise is stated.

The choice of BPMN as the basis for the proposed security extension in this research project, was guided by the following characteristics of BPMN which make it well suited for the purpose of this thesis:

- BPMN is the result of the revision of other business process modelling notations [162].

BPMN emerged as an outcome of a long series of meetings of a large number of business process modelling experts and major software vendors. During these meetings the shapes, which are easily distinguishable from each other and which are well familiar to modelling experts because they appear in other modelling languages, were brought together in the modelling language that was destined to become an industry standard [163].

- BPMN is a graphical notation, which is developed for the facilitation of communication between various stakeholders - end users, business experts, software developers and workflow modellers - involved in the design, development and maintenance of Process-Aware Information Systems [161]. BPMN is easily accessible by technical and non-technical experts alike [160, 164].

- BPMN, according to the evaluation using the Semiotic Quality Framework, is an easy to learn and relatively easy to understand [165].

- BPMN has a rich syntax which allows the modelling of business processes at various levels of abstraction: from the high level of abstraction, which is required when capturing the business view point and mapping the main functionality of a system, to the detailed one, which is required in executable models [17].

- BPMN syntax is rich, but, at the same time, flexible. In the majority of cases, a confined set of BPMN elements suffice [9] (the set of required BPMN elements depends on the modelling purpose and/or target audience). This flexibility makes BPMN even easier to use and learn by a wide non-expert audience, whilst still maintaining the ability to create more detailed specifications of business processes required for execution.

- BPMN offers several types of diagrams for modelling cross-organisational interactions (public processes, collaborations and choreographies). Thus, BPMN allows the representation of cross-organisational interactions at different levels of abstraction [160].

- BPMN is widely adopted in practice [159, 166, 167]. It is the first international standard for business process modelling [159, 161].

- BPMN, due to its expressiveness, allows the modelling of business processes in different scenarios [159, 166, 168]:

    1. Modelling for discovery - fast process capture with process owners, depicts the main details of processes and uses the basic BPMN elements;

2. Modelling for documentation - visualises the main behaviour of a system from the business point of view in greater detail than the above mentioned models;
3. Modelling for analysis (re-design) - adds other behavioural details to the above described models in order to facilitate process analysis and improvement;
4. Modelling for execution - specifies processes with the details required for automated execution;
5. Interaction modelling - represents communication in cross-organisational business processes; and
6. Modelling of semi-structured processes - creates processes for flexible semi-automated execution.

The different use scenarios of BPMN are also discussed in [166]. In this thesis, the focus is on the integration of security into the models developed for purposes others than execution.

- BPMN has formal execution semantics [160] and supports the model-driven engineering paradigm. Although the execution aspect of the proposed security-annotations is out of the scope of this thesis, this is the subject for future research as discussed in Chapter 8.

BPMN is analysed by researchers from various perspectives and compared with other modelling languages. In [169], the comprehensibility of the diagrams expressed in BPMN and UML Activity Diagrams is tested with an audience unfamiliar with the modelling languages. The experiment confirms that BPMN and UML are equally well understood by inexperience readers. In [170], BPMN is compared with the UML Activity Diagram and Extended Enterprise Modelling Language using the Semiotic Quality Framework. In this comparison BPMN scores higher than other notations with BPMN achieving 75% of total marks, while others receiving only around 66%. Another comparative analysis of BPMN and the UML Activity Diagram demonstrates that the languages are very close in terms of effectiveness, efficiency and user satisfaction [171]. In [165], the analysis of BPMN using the Semiotic Quality Framework confirms its comprehensibility appropriateness. In [162], the representational analysis of BPMN is presented. This study confirms that the core set of BPMN elements is effective for the design of concise business process models and that it is easily accessible by business experts.

5.3.2 Types of Diagrams in BPMN

There are different types of diagrams in BPMN [161]:

- Process:
  - Private Non-executable (internal) Business Process - the process which is specific to an organisation and developed for documentation at the modeller-defined level of detail;
  - Private Executable (internal) Business Process - the process which is developed for execution;
  - Public Process - the process which defines the interactions between private business processes and other participants;
- Collaboration - the process which depicts the interactions between two or more business participants; and
- Choreography - the process which defines the expected behaviour between interacting participants.

The main interest of this thesis lies in the weaving of security into public non-executable BPMN models and collaborations because these types of BPMN models are in greater use by business experts. Choreographies and conversations are less popular among non-technical audience targeted by this research project.

5.3.3 BPMN Metamodel and Basic Elements

The metamodel of a business process diagram, which is expressed in BPMN, is presented in Figure 5.1. The syntax of UML class diagram [172] is used to depict the metamodel. The metamodel in Figure 5.1 updates the metamodel of a business process diagram for BPMN 1.0 which is presented in [24, Fig. 1].

Table 5.1 shows the basic BPMN modelling elements.

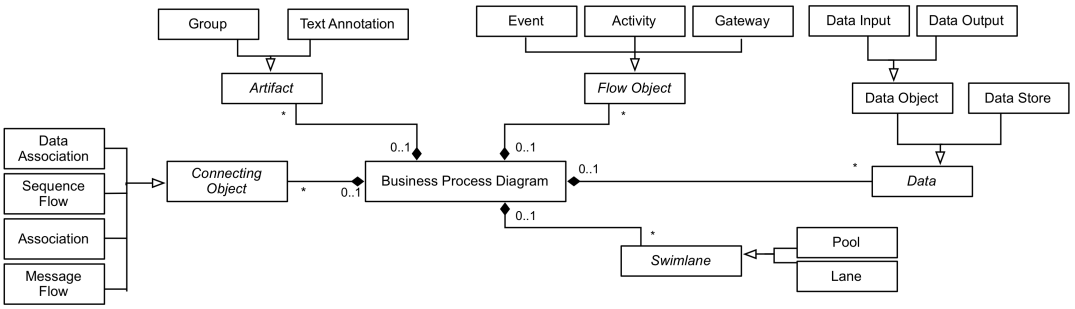


Figure 5.1: The Business Process Diagram metamodel (as described in [161, Sec. 7.3]).

5.3.4 Lack of IAS Modelling Capabilities in BPMN

BPMN, as well as the majority of business process modelling languages, does not allow security modelling by default. It is demonstrated by previous research that the BPMN syntax is insufficient for the representation of security concerns in a clear, unambiguous way. Some security-related details may be presented using the standard BPMN element Text Annotation. However, this way of representing security information lacks clarity and precision, and hinders the usability of security-annotated business process models [24, 25, 38, 173].

In 2012, Altuhhova et al. [25] conducted an analysis of BPMN in terms of its suitability for deriving security requirements and expressing security countermeasures, and aligned BPMN with the domain model of Information Systems Security Risk Management (ISSRM) [59, 174]. The analysis shows that while the BPMN syntax is sufficient for expressing some security-related entities of the risk management domain (e.g. business asset, IS asset, threat, threat agent and attack method), other security-related entities (e.g. security criterion/goal, risk vulnerability, risk treatment and security control) could not be explicitly depicted using the BPMN syntax [25]. The paper concludes that BPMN requires an extension (e.g. the introduction of new constructs) in order to facilitate security modelling [25].

Table 5.1: Basic BPMN Modelling Elements

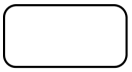
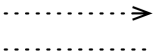
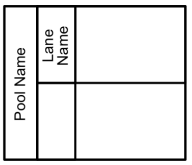
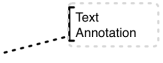
	**Event** - represents something that occurs during a process.
	**Activity** - depicts the action performed by a participant during a process.
	**Gateway** - indicates branching, forking or merging of paths in a process ("if" statement).
	Sequence Flow - depicts the order of activities in a process.
	Message Flow - indicates the flow of messages between the participants of a process.
	**Association** - is used to associate information and artifacts with other BPMN elements.
	**Pool** - represents a participant in a collaboration.
	**Lane** - is a subdivision of a pool and may represent, for example, a department or a specific role within an organisation, a participant of a process.
	**Data Object** - depicts information/documents required during activities.
	**Message** - shows the content of a communication between the participants of a process.
	**Group** - allows grouping of other BPMN elements.
	**Text Annotation** - provides additional information in a model.

Table 5.2: The Alignment of BPMN with the RMIAS

Security concepts extracted from the RMIAS	**Default representation in BPMN/Possible representation in BPMN**	**Visual representation in the existing extensions**
Information Sensitivity	None; Possible: Text Annotation	Menzel et al. [181] - (Table 5.6R); Monakova et al. [166] - (Table 5.6S);
Information State	None; Possible: Text Annotation	Not found
Information Location	None; Possible: Text Annotation	Not found
Security Goal and its Name	None; Possible: Text Annotation	Rodríguez et al. [24] - (Table 5.6A); Sousa et al. [186] - (Table 5.6B); Menzel et al. [181] - (Table 5.6C); Wolter et al. [182] - (Table 5.6D); Varela-Vaca et al. [183] - text annotation; Mulle et al. [21] - text annotation; Saleem et al. [184] - (Table 5.6E); Rekik et al. [96] - text annotation; Altuhhova et al. [185] - (Table 5.6F); Salnitri et al. [152] - (Table 5.6G);
Security Goal Criticality	None; Possible: Text Annotation	Sousa et al. [186] - (Table 5.6I);
Security Countermeasures and its Type	None; Possible: Activity, Group, Association, Transaction, Compensation, Text Annotation	Wolter and Schaad [164] - (Table 5.6J); Wolter et al. [60] - (Table 5.6K); Sousa et al. [186] - (Table 5.6L); Wolter et al. [182] - (Table 5.6D); Varela-Vaca et al. [183] - text annotation; Mulle et al. [21] - text annotation; Brucker et el. [38] - (Table 5.6M); Rekik et al. [96] - text annotation; Monakova et al. [166] - (Table 5.6N); Altuhhova et al. [185] - (Table 5.6O);

In 2012, as a part of this research project, BPMN was aligned with the RMIAS [38]. This analysis, in its extended and corrected version, is summarised in Table 5.2. The last column of Table 5.2 shows whether and how security concepts derived from the RMIAS are represented in the existing security extension. This is discussed in detail in Section 5.4.3. Table 5.2 (columns 1 and 2) examines how the security concepts extracted from the RMIAS[1] could be depicted by the existing BPMN elements and demonstrates that the majority of the security concepts may only be presented

[1]The extraction of security concepts from the RMIAS is discussed in Section 6.1.1

using the Text Annotation BPMN element. However, as already mentioned earlier, the use of text annotations for the representation of the security concepts of different nature is highly likely to lead to misinterpretations.

As Table 5.2 shows, a security countermeasure may be depicted using such BPMN elements as Activity, Transaction, Compensation etc. However, the reuse of the BPMN elements for the visualisation of new concepts is not permitted by the BPMN extensibility rules (Section 5.3.5). Furthermore, it will introduce symbol overload[2] by attaching a new meaning to an existing symbol.

Although any security extension of BPMN should make full use of the existing BPMN elements, there is still a need for new graphical constructs to visualise the key security concepts such as a security goal and its level of criticality, security countermeasure and its type, the sensitivity of information and access permissions for business process participants to different data objects. Thus, the alignment of BPMN with the RMIAS, echoing the conclusions of other researchers in [24, 25], confirms that BPMN requires an extension in order to facilitate information security modelling [24, 25, 38].

5.3.5 Extensibility of BPMN

The inbuilt BPMN extensibility mechanisms make possible the development of domain-specific dialects of BPMN, which still maintain the valid BPMN core [161, Sec. 7.7]. The BPMN extensibility rules are declared in the BPMN specification [161]. Any BPMN-complaint extension should strictly obey these rules.

The BPMN syntax is flexible in the use of size, color, line style, and the positions of graphical elements (except where otherwise is specified). Any extension should aim to retain the "look-and-feel" of BPMN to enable the better readability and understandability of models [161, Sec. 7.7]. Section 2.2.3 of the BPMN international standard [161] allows the following extensions of BPMN:

1. New markers or indicators may be added to an existing BPMN graphical element to highlight the specific attribute(s) of the BPMN element;

[2]Symbol overload happens when the same graphical symbol is used to represented two different semantic constructs. Homographs (the instances of symbol overload) lead to ambiguity and misinterpretations. Symbol overload is regarded as the worst type of anomaly in visual notations [30].

2. A new shape may be added to the BPMN metamodel to represent a new Artifact. The new shape shall not conflict with the existing BPMN graphical elements;

3. A colour may be assigned to a graphical element to extend the information embedded into the element;

4. The line style of a graphical element may be changed as long as it does not conflict with any other line style outlined in the BPMN specification; and

5. The change of the visual appearance of the existing BPMN graphical elements is not permitted.

5.4 Critical Analysis of the Existing Security Extensions for BPMN

5.4.1 Literature Review Methodology

There is a large number of research publications addressing the modelling of security in business processes. There are IAS and risk extensions for various business process modelling languages. Some security aspects are also captured in extensions addressing non-functional requirements in business processes. This thesis does not attempt to provide a comprehensive overview of all research endeavours related to the integration of security into BPM. Even more so because the analysis of many aspects of the integration of security into BPM is already available as discussed in Appendix A.14. In Section 5.4, only closely-related research proposals addressing the representation of security in BPMN are examined.

The selection of security extensions for the analysis initially followed the methodology similar to the one described in Section 2.8.1. A search query was formed out of the following keywords: "Information Security", "Information Assurance", "extension", and "BPMN". The results of the searches formed the initial sample of papers selected for the analysis. Over time the list of the papers grew to include extensions related to the risk management domain, since these extensions consider some concepts which are in the scope of IAS. The list of the papers for analysis was also enriched with the papers recommended by the reviewers and experts with whom Secure*BPMN was discussed in the process of its development. The references in all selected papers were also

traced. Then, it was ensured that all relevant BPMN extensions, which are discussed in the review papers [175, 176, 177, 178, 179, 180] (Appendix A.14), are included in the analysis.

As a general rule, a paper which proposes a security extension for BPMN, whether textual or graphical, was examined in detail. Then, several risk management extensions were also examined because they address security amongst other risk factors. Only the risk-oriented extensions that use the security terminology sufficient for the comparison of these extensions with security extensions were examined. Also the main focus was on the papers that concentrate on(or partially address) the syntax of security-annotations, rather than focus purely on the simulation, validation or execution of security-annotated business processes.

Finally, 15 security and risk extensions for BPMN were selected for the detailed analysis which is presented in the subsequent section.

5.4.2 Discussion of the Existing Extensions

This section contains the detailed discussion of 15 closely related proposals chosen for the analysis. The analysis is summarised in four tables which are discussed in Section 5.4.3.

In addition to this, Appendix A.14 discusses (1) the outcomes of academic reviews of research related to various aspects of the integration of IAS into BPM and (2) mentions other proposals suggesting to integrate security in business process models apart from those selected for a detailed analysis in this chapter.

5.4.2.1 Rodríguez et al., 2007 [24]

Rodríguez et al. [24] propose a BPMN extension which incorporates security into business process models from the business analyst's viewpoint. The need for considering the business analyst's and security expert's viewpoints on security requirements in business processes is acknowledged. The BPMN 1.0 metamodel, which represents the core element of a business process diagram, is extended with five security requirements: Non-Repudiation (NR), Attack harm Detection (AD), Integrity (I), Privacy (P), and Access Control (AC). These security requirements are adopted from [67].

A security requirement is depicted as a padlock symbol with a corresponding capital letter in the center. The criticality of a security requirement on the scale of *low-medium-high* is discussed in

the paper. However, its visual representation is not mentioned.

Rodríguez et al. [253, 14, 152] also suggest an extension for the UML 2.0 Activity Diagram based on a similar logic. In [14], the choice of a padlock symbol for the visualisation of security-related concepts is explained by the strong association between this symbol and the notion of security.

5.4.2.2 Wolter and Schaad, 2007 [164]

Wolter and Schaad [164] suggest an extension for BPMN for capturing authorisation constraints. Authorisation constructs are depicted using the BPMN Text Annotation element enriched with a human figure. An annotation contains a reference (shown in the brackets) to formal constraints on the involvement of users in tasks. For example, the reference *(2,1)* means that the tasks must be performed by different users, while *(1,2)* means that the tasks must be performed by the same user. The extension is evaluated by demonstrating how it may be applied in a BPMN model of a banking workflow.

5.4.2.3 Wolter et al., 2008 [60]

Wolter et al. [60] discuss the importance of security goals in the context of PAIS. According to [60], security goals should be defined by business experts at the business process level while security countermeasures should be identified at the service and resource levels. This thesis, on the contrary, suggests that within a business process model both security goals and security countermeasures (along with other security information) must be depicted to provide an holistic view of security in the process.

Wolter et al. [60] discuss a set of security goals including confidentiality, integrity, authentication, authorisation, traceability and auditing, and availability without making any reference to how or from where this set of goals is derived. The syntax of the proposed extension is not discussed. However, in order to evaluate the proposal, one sample BPMN diagram annotated with security information is presented. The example depicts only security countermeasures such as binding of duty, separation of duty, encryption and the signing of a contract. A security countermeasure is depicted using the Text Annotation element, which shows the name of a countermeasure and is enriched with an icon presumably indicating the nature of the countermeasure. None of the security goals discussed in the paper are represented.

5.4.2.4 Souza et al., 2009 [186]

Souza et al. [186] present Sec-MoSC (Security for Model-oriented Service Composition), a methodology for the annotation of BPMN models with security abstractions and for the translation of annotated models into BPEL process specifications enforced at runtime. A range of security goals and countermeasures is identified (see Table 5.5) for service composition in the context of a Virtual Travel Agency.

BPMN is extended with three elements: NF-Attribute (security goal), NF-Statement (the criticality of an activity), and NF-Action (security countermeasure), where NF stands for *non-functional*. A security goal is depicted as a cloud shape with the name of the goal inside. A security goal is attached to an Activity element. The criticality of an activity is depicted as a padlock at the corner of the Activity element.

Only technical countermeasures, executable at runtime, are considered. They are depicted as the names of NF-Action functions inside the Pool BPMN elements. In this proposal, symbol overload occurs because of the reuse of a Pool element to represent a security countermeasure.

An Eclipse plug-in and a translator converting annotations into executable XML configurations are presented [186].

5.4.2.5 Menzel et al., 2009 [181]

Menzel et al. [181] suggest an extension for BPMN for the specification of security requirements in business processes with the purpose of their automatic translation into a concrete security configuration in the context of SOA. The paper discusses the following security goals: authentication, authorisation, trust, data confidentiality and integrity, system integrity and availability. No reference is found in the paper describing from where or how these security goals are derived.

An example of an annotated model of an ordering process is provided. The syntax of the proposed extension to BPMN includes the following graphical elements: asset value, trust and security goal. Asset value is depicted as a padlock symbol inside a Data Object or an Activity element. The level of the filling of a padlock symbol indicates the rating of the asset value on the scale from negligible to extreme. In an annotated example, it is hard to distinguish the value of an asset because the icons are too small. The trust between the participant of a process is depicted as a Data Object with a handshake icon. Hence, a symbol overload occurs because an existing BPMN element is reused

to represent the concept of trust. Another reuse of a BPMN element is encountered when a Group element depicts a security goal as applied to a group of activities. The type of security goal in this instance is not visually indicted. The paper also shows the sample XML configuration for message encryption.

5.4.2.6 Wolter et al., 2009 [182]

Wolter et al. [182] introduce a model-driven transformation framework for generating security configurations from security-annotated business process models. For this thesis, the tool which in the proposed transformation framework supports the graphical annotation of business process models is of interest.

The paper addresses four security goals, namely authorisation, authentication, confidentiality and integrity. The goals are chosen at the authors' discretion stating that these goals "*have the most significant effect on the modelling of business processes and people involved.*"

The paper presents one annotated sample diagram expressed, presumably, in BPMN 1.0 (the paper itself does not mention which modelling notation is used). The business process modelling notation is enriched with several graphical security elements of which only one - four-eye principle - is discussed in the paper. The four-eye principle is depicted as an icon with two human figures placed within a BPMN Text Annotation element. For evaluation purpose it is demonstrated how an XACML policy is generated from an annotated model.

5.4.2.7 Mülle et al., 2011 [21]

Mülle et al. [21] propose a language for the formulation of security constraints embedded in BPMN. The authors attempt to address two gaps in the research: (1) the incompleteness of the security modelling vocabulary and (2) insufficient user involvement. The proposed language uses the standard BPMN Text Annotation element as a container for security constraints.

The basis of the language is formed by the following requirements: authorisation, authentication, auditing, confidentiality, data integrity, security-specific user involvement and trust-specific aspects. The authors also propose a new approach to the transformation of security annotations into the representation, supported at process execution. The paper significantly extends the set of

security requirements being addressed. Nevertheless, the limitations of the work is in deriving security requirements from only two specific scenarios originating from the employability domain. Although the scenarios are complex, it is not sufficient evidence to support the statement about the completeness and general suitability of the identified security requirements. For example, essential security goals such as availability and accountability are omitted.

The main aim of the proposed language is to translate security requirements (annotations) specified in a BPMN model into an executable specification. Hence, the language is text-based and oriented on technical experts. Business experts would find the annotations hard to comprehend. This would deter business experts from the security-annotation of business process models and complicate security requirements gathering. The similar text-based BPMN extension for privacy-aware business processes is presented by the same group of authors [187].

5.4.2.8 Varela-Veca et al., 2011 [183]

Varela-Veca et al. [183] develop a framework for weaving risk into BPM. They extend BPMN with the risk information expressed in the textual form using a Text Annotation BPMN element. Varela-Veca et al. [183] focus on the diagnoses of non-conformance of security objectives in annotated models. The constructs introduced into the BPMN metamodel are extracted from the UML profile for modelling quality of service and fault tolerance characteristics and mechanisms [254].

5.4.2.9 Brucker et. al., 2012 [38]

Brucker et. al. [38] suggest the SecureBPMN methodology, which allows the modelling of security requirements at the system design stage along with the functional requirements and the enforcement of the requirements at run-time. The security requirements considered in [38] are limited to access control, separation of duty, binding of duty and need-to-know. The requirements are derived from a travel-approval process and from other unnamed case-studies. The main criticism of this proposal is associated with the fact that it focuses on Role Based Access Control (RBAC) and overlooks other security concerns. The proposal does not outline an extended BPMN metamodel. Brucker et. al. [38] extend the Activity Designer with security modelling capabilities and enable the generation of XACML policies from annotated BPMN models.

The importance of a clear visual representation of security requirements within BPMN model is acknowledged. It is said that security aspects should be embedded into BPMN in a well-arranged

manner. However, there is no discussion or justification provided regarding why the symbols suggested in the paper are clear and well-arranged, and why the representation suggested is better than others previously proposed.

An analysis of the syntax proposed in [38], shows that it introduces symbol overload: (1) it uses a rectangle with rounded corners to represent a security requirement, while it already represents an Activity and (2) it uses a solid line arrow to represent the applicability of a security requirement to an Activity, while it is a Sequence Flow BPMN element.

5.4.2.10 Saleem et al., 2012 [184]

Saleem et al. [184] develop a BPMN security extension for SOA applications. In comparison with [24], only a limited set of security requirements is considered: confidentiality, integrity and availability (associated with non-repudiation). The main criticism of this proposal is associated with the use of an outdated metamodel of BPMN for extension. This proposal extends the metamodel of BPMN 1.0 with security constructs. However, the metamodel of BPMN 2.0, which emerged in 2011, is different.

A set of graphical notations for confidentiality, integrity and availability is also introduced. The proposed symbols do not comply with the BPMN extensibility rules as they do not maintain the "feel-and-look" of BPMN. Despite its limitations, this work is one of a few which discusses, although very briefly, a rationale for its syntax.

5.4.2.11 Monakova et al., 2012 [166]

Monakova et al. [166] describe a tool-supported framework for modelling and monitoring security and safety requirements in supply chains. Monakova et al. [166] consider the following security controls: signature, encryption, audit-control, privacy-policies and separation of duties.

The syntax of the proposed extension includes tags for (1) logical and physical assets (an icon inside a rhombus shape attached to a Data Object) and (2) security controls (as icon placed inside a hexagon attached to Data Object and Activity BPMN elements).

A software prototype is presented. Although the paper states that it aims to improve comprehension through the visualisation of security concepts, the syntax of the notation is not justified or

analysed in any way. The proposal does not concentrate on IAS as such, but considers it as one of the aspects among other security and safety requirements.

The proposal is developed to suit the needs of food supply chains and is not broadly applicable. According to the paper, the software tool was presented to and discussed with supply chain stakeholders and received positive feedback. However, the description of the evaluation process and of the results is limited to the statement above and no further details are provided.

5.4.2.12 Rekik et al., 2012 [189]

Rekik et al. [189] extend BPMN for security modelling in a cloud environment. The following security requirements are addressed: integrity, privacy, access control, non-repudiation, availability and audit. The requirements are derived from Rodríguez et al. [24] as they are said to be pertinent to a cloud environment. The concept of inter-sides communications is also introduced in the extended BPMN metamodel. The syntax of the proposed extension is not discussed. All security annotations in the example diagram are depicted using the Text Annotation BPMN element.

5.4.2.13 Marcinkowski and Kuciapski, 2012 [173]

Marcinkowski and Kuciapski [173] introduce an extension for risk handling in BPMN 2.0. The semantics are derived from risk management standards. The following risk modelling elements are incorporated into BPMN: risk factors, risk types, risk handlers and risk mitigation methods. One example diagram is presented illustrating the application of the proposed method to the process of managing an architectural contest. Risk in the diagram is depicted as a triangle with an exclamation mark inside. No discussion of the syntax is provided.

5.4.2.14 Altuhhova et al., 2013 [185]

Altuhhova et al. [185] propose a security risk-aware BPMN extension based on the Information Systems Security Risk Management (ISSRM) domain model [59]. The following security elements are introduced into BPMN to enable security/risk annotation:

- The characteristic of an asset - a circle with a corresponding letter inside (B for a business asset and IS for an IS asset) which is applied to the top right corner of the Event, Gateway and Task BPMN elements;

- Security constraint - a padlock symbol which may be accompanied by a text annotation and is attached to the bottom right corner of BPMN elements;
- Security objective/goal - a padlock symbol (three security goals, namely confidentiality, integrity and availability are addressed);
- Security criterion - a BPMN Text Annotation;
- Risk - a combination of an event and impact;
- Vulnerability - a black square which may be attached to the bottom right corner of the Activity and Data Store BPMN elements, and may be accompanied by a text annotation;
- Impact - an unlocked padlock symbol at the bottom right corner of the Data and Activity BPMN elements; and
- Other security elements such as event, target, threat, threat agent, attack method, associations between security elements - depicted using the existing BPMN elements.

The proposed notation is used to depict the characteristics of assets, specify security objectives and model violation scenarios. Based on the analysis of annotated diagrams, diagrams are corrected using the BPMN syntax to include actions which are required to minimise the risk of violations.

Several annotated BPMN diagrams of the activities of an Internet store are presented to support the validity of the proposal. The proposal is evaluated with regard to its semiotic clarity, which requires a one-to-one correspondence to be ensured between a visual element and a semantic construct. The analysis reveals that all four possible deficiencies, namely redundancy, overload, incompleteness and excess occur in the suggested extension. The paper reports that the proposed extension was used in student exercises. No details of the exercises or results are discussed in the paper. The extension is also used to derive risk-oriented patters in [255].

5.4.2.15 Salnitri et al., 2014 [152]

Salnitri et al. [152] propose SecBPMN enabling security annotations. The security goals to be woven into business process models are derived from the RMIAS [96], which is presented in Chapter 3 of this thesis. The choice of the RMIAS is explained by the fact that it introduces the most comprehensive set of security goals [152]. Thus, in [152], the RMIAS and, more specifically, the IAS-octave, found its application in business process modelling research independently of the

author of this thesis. This confirms, first, the validity of the RMIAS as a model of the IAS domain and, second, its suitability as the basis for the semantics of a security modelling extension for a business process modelling language.

SecBPMN proposes a syntax for each of eight security goals adopted from the RMIAS. Each symbol is an orange circle with an icon inside the circle. However, the circle with an icon inside it already represents an Event in BPMN. This design decision is hardly optimal as it introduces symbol overload. With existing difficulties in BPMN regarding the distinguishing of a large number of Event symbols, the reuse if this symbol to represent a security construct may complicate matters to a state where an annotated model will become unreadable. The syntax of SecBPMN is said to be guided by the Theory for Visual Notations Design [30]. The paper provides a brief (four sentences) discussion of the syntax. The icons are developed with the help of security experts, however, no details of the process or justification of the chosen icons is given.

The paper also proposes SecBPMN-Q, a query language for expressing security policies. The proposal is verified in a case-study.

5.4.3 Extensions Analysis Summary

Tables 5.3, 5.4, 5.5 and 5.6 summarise the analysis of the discussed extensions.

Table 5.3 provides an overview of the extensions. It shows the purpose of each proposal, the version of BPMN used, the target audience and the basis for semantics. It also shows whether the syntax of an extension is textual or graphical and outlines the guidance for the syntax design exploited in the analysed source.

Table 5.4 continues the overview of the extensions. It shows the domain for which an extension is developed or where its application is exemplified. The table outlines how each extension is evaluated. It also shows whether tool support for the proposed annotation method is provided and whether inter-organisational security is addressed.

Table 5.3: The overview of the extensions

Authors [ref.] Year	Purpose	BPMN Version	Target audience	Basis for the semantics	Syntax, guidance for syntax
Rodriguez et al. [24] 2007	to incorporate security requirements into business process models from bysiness analyst perspective	1.0	business analyst and security expert	from [67]	Graphical, not discussed
Wolter and Schaad [164] 2007	to depict authorisation constraints	1.0	workflow modellers	authorisation constraints chosen from the literature at the authors' discretion	Graphical, not discussed
Wolter et al. [60] 2008	to enable business experts to define security goals at business level	1.0	business experts	not specified	Graphical, not discussed
Sousa et al. [186] 2009	to cover transition from the requirements stage through modelling to executable stage	1.2	business and security experts	requirements for specific case study	Graphical, not discussed
Menzel et al. [181] 2009	to describe security requirements in business process models and facilitate the generation of security configurations	1.0	IT audience	not specified	Graphical, not discussed

Continued on the next page

Table 5.3 – *Continued from the previous page*

Authors [ref.] Year	Purpose	BPMN Version	Target audience	Basis for the semantics	Syntax, guidance for syntax
Wolter et al. [182] 2009	to enable security and business experts to define security goals collaboratively; to generate technical system policies	1.0	business and IT security experts	not specified	Graphical, not discussed
Varela-Vaca et al. [183] 2011	to diagnose non-conformance of security objectives	1.2	business expert and risk analyst	extracted from [254], ISO/IEC 27004	Textual, N/A
Mülle et al. [21] 2011	to transform into executable specifications	2.0	software developers and security experts	identified from the employability domain	Textual , N/A
Saleem et al. [184] 2012	to enable business process experts to specify security goals	1.0	business process and security experts	chosen from the literature at the authors' discretions	Graphical, the rational of the symbols design is explained
Brucker et el. [38] 2012	to generate security policies from annotated business process models and enforce them	2.0	software developers	identified from case-studies	Graphical, not discussed
Rekik et al. [189] 2012	to specify security requirements in business processes outsourced in the cloud	2.0	business analyst and/or security expert	adopted from [24] 2012	Textual , N/A
Marcinkowski and Kuciapski [173]2012	risk management	2.0	risk analysts	from risk management literature	Graphical, not discussed

Continued on the next page

Table 5.3 – *Continued from the previous page*

Authors [ref.] Year	Purpose	BPMN Version	Target audience	Basis for the semantics	Syntax, guidance for syntax
Monakova et al. [166] 2012	to allow a business user to specify security and safety requirements	2.0	business experts	from a motivating supply chain scenario	Graphical, not discussed
Altuhhova et al. [185] 2013	to develop security requirements to secure important assets	2.0	system analysts	ISSRM [59]	Graphical, TVND [30]
Salnitri et al. [152] 2014	to model and verify the compliance of a business process model with security policies	2.0	business process modeller	RMIAS [96]	Graphical, TVND [30]
Secure*BPMN	to facilitate the discussion of IAS issues in multi-disciplinary teams	2.0.1	multi-disciplinary team of experts	RMIAS [96]	Graphical, TVND [30]

Table 5.4: The overview of the extensions (part 2)

Authors [ref.] Year	Domain	Evaluation	Tool Support[3]	Inter-org. Aspect
Rodriguez et al. [24] 2007	Healthcare- Patient Admission	annotated example	No	Yes
Wolter and Schaad [164] 2007	Banking	annotated example	No	No
Wolter et al. [60] 2008	banking (open an account)	annotated example	No	Yes
Sousa et al. [186] 2009	Virtual Travel Agency	annotated example and tool supporting the transformation	Yes	No
Menzel et al. [181] 2009	Order process	annotated sample BPMN diagram of an order process, resulting XML configuration	No	Yes
Wolter et al. [182] 2009	Financial check	annotated sample diagram and tool generating XACML policies	Yes	Yes
Varela-Vaca et al. [183] 2011	Healthcare- Patient Admission	sample annotated diagram and mathematical calculation of risk for the scenario	No	No
Mulle et al. [21] 2011	Employability Domain	two annotated diagrams and transformation into XACML policies	No	Yes
Saleem et al. [184] 2012	Online student Information System	annotated example	No	No
Brucker et el. [38] 2012	Travel approval process	sample annotated diagram and tool supporting modelling and transformation	Yes	No
Rekik et al. [189] 2012	University admission	annotated example	No	Yes
Marcinkowski and Kuciapski [173] 2012	Managing Architecturel Context	annotated example	Yes	No

Continued on the next page

Table 5.4 – *Continued from the previous page*

Authors [ref.] Year	Domain	Evaluation	Tool Support	Inter-org. Aspect
Monakova et al. [166] 2012	Supply chain	software prototype and discussions with experts	Yes	No
Altuhhova et al. [185] 2013	Internet store	annotated diagrams, students exercise, development of risk patterns	No	No
Salnitri et al. [152] 2014	ATM	annotated example, case-study	Yes	No
Secure*BPMN	Translation company (SME)	annotated examples, analytical evaluation of ontological completeness and cognitive effectiveness, empirical evaluation of the overall effectiveness with end-users	Yes	Yes

Table 5.5 indicates which security goals and countermeasures are addressed, while Table 5.6 shows which security constructs are visually represented in the extensions examined.

The last row of Tables 5.3, 5.4, 5.5 and 5.6 shows Secure*BPMN for the comparison which is drawn at the end of Chapter 7 in Section 7.5.

5.4.3.1 Basis for the Semantics

While analysing the security extensions, first, the bases for their semantics are examined. In each paper, it is identified which security concepts are introduced into BPMN, and how or where from these concepts are derived. Table 5.3 (column Basis for the semantics) shows that some proposals do not provide any discussion on why they introduce in BPMN the proposed set of security elements, while others extract security requirements from the IAS literature at their discretion [60, 181, 182, 183, 184]. The justification of a requirement, if any is provided, is usually limited to a brief outline of its importance either within the IAS domain in general or in the context of a specific scenario. However, none of these papers tested whether the set of the requirements they

consider is comprehensive or whether an extension covers all security concepts relevant to a scenario. None of these papers provides a reason for not including overlooked key security concepts.

Another group of papers derives security concepts (mainly security goals and countermeasures) from other publications. Varela-Vaca et al. [183] adopt requirements from ISO/IEC 27004. Rodríguez et al. [24] extend BPMN with a set of security requirements extracted from Firesmith [67]. Rekik et al. [96] and Saleem et al. [184] use the requirements from Rodríguez et al. [24]. However, although Firesmith [67] provides a broad list of security requirements, not all of them are adopted by Rodríguez et al. [24] (e.g. requirements such as physical protection, confidentiality, anonymity, recovery and prosecution, which are discussed in [67], are not addressed in [24]). While Firesmith [67] approaches IAS holistically and considers factors beyond technical ones (e.g. personnel integrity and physical protection are discussed), when his taxonomy of security factors is adopted in these three BPMN security extensions [24, 96, 184] only a limited set of factors is introduced into BPMN. By omitting some of security factors, these extensions lose the holistic approach to IAS and confine themselves to addressing only technical security issues.

Salnitri et al. [152] adopt the RMIAS as the basis for the semantics of the extension. Although Salnitri et al. [152] use the complete set of security goals from the RMIAS (the IAS-octave), the security concepts of other dimensions of the RMIAS are ignored. No discussion is provided as to why other security concepts which are explicit in the RMIAS are not visually represented by the extension.

The most thorough in terms of its semantics is the extension proposed by Altuhhova et al. [25, 185], who elaborate the extension based on the ISSRM [59]. The ISSRM is developed as a part of a PhD project. It is based on an extensive literature analysis and is evaluated via interviews with nine security experts and student exercises. There is some overlap between the concepts covered by the RMIAS and the ISSRM (Table 5.6). Nevertheless, these models cover adjacent, but different domains. The RMIAS and ISSRM differ reflecting the specifics of the domains their represent and the range of literature analysed during the model development process. The ISSRM is not presented as a reference model, but as a concepts and relationships diagram. Thus, while specifying the key concepts of the risk management domain it does not go as far as the RMIAS in identifying the taxonomies of possible values for each concept (e.g. the list of security goals, the types of security countermeasures and the information taxonomy).

As Table 5.3 indicates, several extensions derive security requirements from specific domains or case studies [21, 38, 166, 186, 187]. Hence, the applicability of these extensions is limited to those

domains (e.g. the extension in [166] is designed for food supply chains).

The security goals are modelled in the majority of the extensions (Table 5.6). Some papers (e.g. [60, 182]) discuss the critical importance of the notion of a security goal for business experts and state that there must be a way for business experts to specify security goals in a business process. While acknowledging the importance of security goals to be represented in business processes, the extensions, echoing the problem observed in the IAS literature in general, are in disagreement about the set of goals to be considered. They outline various and, as discussed above, often unjustified sets of security goals (Table 5.5).

Table 5.5: Security Goals and Countermeasures addressed by the Analysed Security Extensions.

Authors [Ref.]	Confidentiality	Data Integrity	Availability	Authentication	Authorisation	Traceability	Auditing/Auditability	Non-repudiation	Attack Harm Detection	Privacy	Access Control	Security Permissions	Security Role	Data Retention	Restricted Access	Data Sharing	Service Certification	Monitoring	Authenticity/Trust/Trustworthiness	System Integrity	Safety	Data & Message Security	User Involvement	Accountability	Separation of Duty	Binding of Duty	Need to Know
Rodriguez et al. [24]		X						X	X	X	X	X	X														
Wolter and Schaad [164]					X																				X		
Wolter et al. [60]	X	X	X	X	X	X	X																				
Sousa et al. [186]	X	X		X			X				X			X	X	X	X	X									
Menzel et al. [181]	X	X	X	X	X														X	X							
Wolter et al. [182]	X	X		X	X																						
Varela-Vaca et al. [183]	X	X	X																								
Mulle et al. [21]	X	X		X	X		X															X	X				
Saleem et al. [184]	X	X	X			X	X																				
Brucker et el. [38]											X														X	X	X
Rekik et al. [189]		X	X					X		X	X																
Marcinkowski and Kuciapski [173]																											
Monakova et al. [166]							X			X											X				X		
Altuhhova et al. [185]	X	X	X																								
Salnitri et al. [152]	X	X	X				X	X		X									X	X				X			
Secure*BPMN	X	X	X	X	X		X	X		X	X	X	X		X	X	X	X	X	X		X		X	X	X	X

Note: X - addressed by the extension.

The majority of the extensions analysed visualise only security goals and countermeasures [14, 21, 24, 38, 60, 152, 164, 182, 184, 38]. However, the extensions do not clearly distinguish security goals (*what* must be achieved) from security countermeasures (*how* it may be achieved). The papers outline the lists where security goals are mixed with countermeasures. Table 5.6 indicates that only two of the extensions examined [185, 186] depict security goals and countermeasures using different graphical elements.

Six out of the papers analysed demonstrate the application of their extensions to BPMN collaboration diagrams. However, the inter-organisational security issues are not explicitly discussed. The extensions deal with access control, but only within the scope of one organisation (e.g. [38]). The access permissions of business process participants, if they are discussed in the paper, usually have no graphical representation. They are expressed either via textual annotations [24] or as the visually-hidden parameters which are later used for the creation of executable configurations [38].

The analysis of the semantics of the extensions examined confirmed the lacks of an agreed, shared understanding of IAS in the context of secure business process design. Section 1.6 of this thesis stated that the research presented in this thesis was conducted in an iterative manner. When the security extensions for BPMN and other modelling languages were examined at the beginning of the project, the absence of a solid basis for the semantics and the lack of clarity regarding security concepts to be introduced in business process modelling languages were encountered. These problems prompted the detailed investigation into the IAS domain, which is summarised in Chapter 2. As Chapter 2 demonstrated, no generally-agreed approach to IAS or an up-to-date, comprehensive and well-justified conceptual model of the domain were found in the IAS literature either. This, in turn, impelled the development of the RMIAS.

The semantics of the extensions are granular. The expression of security goals by business experts is isolated from the selection of security countermeasures which helps to achieve those goals (cf. [60]). Only a few proposals [166, 181] enable the marking of Data Objects in a business process model according to their value or sensitivity (Table 5.6). Table 5.2 shows whether security concepts derived from the RMIAS are represented in the existing security extensions. This analysis confirms that not all security concepts of the RMIAS are visualised in the extensions examined. None of the extensions address all of the RMIAS security concepts.

The extensive use of business process models for automation within the model-driven software engineering approaches often leaves in the shadow the use of BPMN outside software development, e.g. for documentation, communication and analysis (an overview of the Model-Driven Engineering (MDE) is presented in Appendix A.15). The security extensions analysed are mostly follow the MDE paradigm since they are used for the elicitation of technical, enforced at run-time, security requirements.

As a result of the adopted MDE approach, an holistic approach to IAS as a complex managerial issue that goes beyond computer and network security, and electronic data protection is often absent in the extensions examined. Business experts, who are involved in the design of secure

business processes, are not interested in the development of secure software, secure networks or secure SOA only. Their main interest is overall business security, which could only be achieved through a sensible combination of technical, legal, organisational and human-oriented security countermeasures. However, the BPMN extensions examined do not provide for modelling IAS in this broad sense. Moreover, the extensions analysed mention only the need to involve business experts, while the need to involve experts in other domains is not discussed.

5.4.3.2 Syntax

As Table 5.3 shows, the majority of the proposals pay little or no attention to their syntax. The syntax is often not discussed or justified. The design of graphical elements is usually guided by the pure intuition of developers. Some security extensions exclusively use a Text Annotation BPMN element to represent security information in a business process model. However, this is the method of low clarity, precision and effectiveness (Section 5.3.4).

The lack of attention to the syntax of security extensions may be attributed to two reasons. The first reason is that the theory for the design of cognitively effective syntax was proposed only recently. In 2009, Moody, the author of the Theory for Visual Notation Design (TVND), while introducing the TVND wrote: "*Currently, in evaluating, comparing and constructing visual notations we have little to go on but intuition and rule of thumb: we have neither theory nor a systematic body of empirical evidence to guide us*" [30].

Over the last several years, the importance of the cognitive effectiveness of the syntax of security extensions began to acquire recognition among researchers. Two of the recently proposed extensions [185, 152] declare that they follow the TVND [30]. However, these extensions discuss the syntax only at a superficial level. It is not discussed in the papers how and which principles are obeyed and to what degree, and what trade-offs are made between the principles. None of the papers provides a detailed analysis of the syntax in terms of the principles of the TVND.

The second reason is the model-driven engineering context in which the proposed extensions are developed. Since the main purpose of the majority of the extensions analysed (e.g. [38, 60, 181, 186]) is the transformation of security requirements expressed in business process models into security configurations which may be executed by workflow management systems, the visual representation of security constructs and their clarity to humans is secondary for the extensions' developers. Although the authors of the extensions try to involve business users in the security-

annotation of business processes, the fact that annotated models are primarily destined for automatic transformation, rather than for understanding/communication, negatively affects the clarity of the syntax making it hard to comprehend for humans. The main emphasis is often made on the transformation of annotation into code and on the tools enabling this transformation, while very little effort is put into the design of a clear intuitive syntax, compliant with BPMN extensibility rules and with the scientific principles of the design of cognitively effective notations.

Table 5.6 shows the security constructs which are graphically represented by the examined extensions.

Table 5.6: Visual Constructs in the Security Extensions Analysed

An empty cell means that the construct is not visualised in the source.

A letter(s) in a cell indicates that the construct is visualised in the source. Below the table, for each letter(s) there is a description explaining how the construct is visualised in the source.

Authors [Ref.]	Security Goal and its Type	Security Goal Criticality	Security Countermeasure and its Type	Information Form	Information Sensitivity	Information State	Information Location	Access Permissions	Risk	Trust	Vulnerability/Threat	Impact
Rodríguez et al. [24]	(A)							TA				
Wolter and Schaad [164]			(J)									
Wolter et al. [60]			(K)									
Sousa et al. [186]	(B)	(I)	(L)									
Menzel et al. [181]	(C)				(R)					(Z)		
Wolter et al. [182]	(D)		(D)									
Varela-Vaca et al. [183]	TA		TA						TA		TA	
Mulle et al. [21]	TA		TA									
Saleem et al. [184]	(E)											
Brucker et el. [38]			(M)									
Rekik et al. [189]	TA		TA									
Marcinkowski and Kuciapski [173]									(X)			
Monakova et al. [166]			(N)		(S)							
Altuhhova et al. [185]	(F)		(O)						(Y)		(AA)	(BB)
Salnitri et al. [152]	(G)											
Secure*BPMN	(H)	(H)	(P)	(Q)	(T)	(U)	(V)	(W)	(CC)	(DD)		

Comments for Table 5.6:

TA - a textual annotation (no graphical representation);

(A) - a padlock with the initial letters of the security goals name inside;

(B) - a cloud shape with the name of the security goal;

(C) - a dashed line depicts a security group, the type of a goal is not visually indicated;

(D) - an icon (padlock) within an annotation element;

(E) - an icon over BPMN connector;

(F) - a padlock with the initial letters of the security goals name inside;

(G) - a circle with an icon inside;

(H) - a circle-based shape derived from a target symbol where the filling of the shape indicates its criticality, while the letters in the middle of the shape point out to the goals name (Secure*BPMN);

(I) - a padlock at the bottom right corner of an activity element;

(J) - a text annotation with a human figure icon;

(K) - a text annotation enriched with an icon indicating the type ;

(L) - a pool with the name of secuirty control function inside dotted line;

(D) - an icon indicating the type placed within an annotation element;

(M) - a BPMN activity element enriched with an icon at the top part of an element;

(N) - an icon indicating the type inside a hexagon;

(O) - a BPMN activity element;

(P) - a (blue) padlock symbol with a semantically transparent icon in the middle which indicates the type of a countermeasure (Secure*BPMN);

(Q) - a semantically transparent icon positioned at the right top corner of a Data Object, Data Store or Message BPMN element (Secure*BPMN);

(R) - a padlock filled with black according to the asset value placed at the bottom right corner of a data object;

(S) - an icon in a rhombus shape attached to data object;

(T) - a pentagon filled with colour and a certain number of exclamation marks to indicate the level of sensitivity and placed at the bottom left corner of a Data Object, Data Store or Message BPMN element (Secure*BPMN);

(U) - derived based on the position of an element in a diagram and not visually indicated - no corresponding image (Secure*BPMN);

(V) - a textual marker placed at underneath the Swimlane name (Secure*BPMN);

(W) - a pentagon shape filled with colour and a certain number of exclamation marks positioned on the right-hand side of the Swimlane name (Secure*BPMN);

(X) - a triangle with an exclamation mark inside;

(Y) - a combination of BPMN and security elements;

(Z) - a BPMN data object with a handshake icon inside;

(AA) - a red square accompanied by a text annotation and placed at the bottom right corner of a BPMN element;

(BB) - an unlocked padlock;

(CC) - indicated by the criticality of a security goal (Secure*BPMN); and

(DD) - indicted by the security goal Authenticity/Trustworthiness (Secure*BPMN).

Confirming the importance of the cognitive effectiveness of security extensions, Leitner et al. [177] tested the clarity of the graphical symbols suggested in six BPMN extensions (these six extensions are analysed in this thesis). The analysis concludes that the suggested symbols are not optimal in terms of their design and are often found hard to interpret by an audience inexperienced in security [177]. The analysis of the syntax of security extensions, which is revealed in this chapter, also infers that many of the proposed extensions are not optimal in terms of their syntax design and may be improved. The inference above further confirms that pure intuition and common sense do not always lead to optimal design decisions [188]. For example, as discussed in the previous section, many extensions reuse the existing BPMN elements. By doing so they introduce symbol overload. Although, intuition and common sense may lead to the decision to reuse the existing symbols in order to reduce complexity, the scientific evidence summarised in the TVND [30] proves that symbol overload is the worst deficiency in the syntax design and leads to misinterpretation and confusion.

While obeying the principles of the design of cognitively effective notations, developers must also strictly obey the BPMN extensibility rules. However, this is not always the case. Section 2.2.3 of the BPMN international standards [161] states that a new graphical element "*SHALL NOT conflict with the shape specified for any other BPMN element or marker*". Despite this restriction, as discussed in the previous section, some extensions reuse BPMN elements and assign to them new meaning (e.g. in [38] - the Activity and Sequence Flow elements, in [152] - the Event element, in [181] - the Data Object, in [186] - the Pool element). By reusing BPMN elements, these extensions not only introduce symbol overload, but also break the BPMN extensibility rules.

5.4.3.3 Evaluation

The evaluation of newly proposed design methods is in general addressed in a very confined form (the difficulties and scarcity of the evaluation of IS design methods are discussed in [37]). Reflecting on the decade of BPM research, Van der Aalst [11] points out a failure to present equally well in a paper a newly proposed modelling technique and its analysis or evaluation. The trend of an insufficient attention to the evaluation of new methods also holds for security extensions for business process modelling languages.

As Table 5.4 (column Evaluation) shows, the evaluation of the proposed security extensions is performed only in a small number of papers examined.

The evaluation of the proposed extensions in many cases [24, 60, 184, 189, 173, 164] is limited to presenting a BPMN diagram annotated using the proposed method (Table 5.4). In reality, the annotated example only demonstrates that it is graphically possible to annotate a BPMN model in a suggested way. It proves neither the cognitive effectiveness of the proposed icons (or, at least, it is left to be judged by the reader), nor the usefulness or ease of use of the proposed method, nor the overall effectiveness of the proposed method.

Other papers mention that case-studies [152], student exercises [185] and discussions with experts [166] were used for evaluation. However, no details of these evaluation activities or their results are provided in either of the papers. Even the number of people who were exposed to an extension is not typically stated. The description of evaluation is confined to the acknowledgement of the fact that evaluation activities were undertaken.

Other proposals [21, 38, 186, 181, 182, 163, 186] are evaluated via the development of a software tool or framework that enables the generation of executable security configurations, usually expressed in XML-based languages. This method of evaluation stems from the model-driven paradigm. There is a logical deficiency in this type of evaluation. Using this logic any extension, irrespective of the set of security concepts it represents (semantics) and irrespective of graphical elements it uses (syntax), is valid as long as it is possible to transform it into executable policies.

It is clear that these papers aim to produce executable policies. However, they all state that their main purpose is to involve business experts in security requirements gathering. With this purpose in mind, the syntax and its clarity to business experts must become a priority. Despite this, none of the papers analysed attempt to analyse to what degree the set of security concepts the proposal addresses is comprehensive and suitable for its target audience. None of the papers evaluate the

cognitive effectiveness of syntax either analytically or with end users. Although in [152] it is mentioned that some experts were involved in the design of symbols, no details of the discussions are provided. In none of the papers analysed the overall effectiveness of a proposed annotation technique is empirically tested (for example using existing method such as the Method Evaluation Model [136]).

The number of security extensions which emerged in the last several years confirms the need for a security extension for BPMN. Despite the existence of several proposals, their critical analysis which is contained in this chapter shows that there is still a room for numerous improvements in terms of semantics, syntax and evaluation.

5.5 Chapter Summary

This chapter explained the approach to BPM adopted in this thesis. The choice of BPMN as the business process modelling language to be extended with security elements in this research projects was advocated. A detailed analysis of the existing security extensions for BPMN was outlined.

The established deficiencies of the existing extensions, which are discussed in detail in the preceding section, are recapitulated below:

- The semantics suffers from granularity, inconsistency and incompleteness. There is no extension that would allow the simultaneous modelling of security goals, security countermeasures, the characteristics of information and access permissions at inter-organisational level. Security goals are not distinguished from security countermeasures.
- The semantics of the extensions is weakly justified. The security concepts which are introduced in business process models are often chosen at the authors' discretion. The justification is confined to a discussion of the relevance of a concept to the IAS domain. The completeness of the suggested set of concepts is not discussed as well as the reasons for the non-inclusion of other key security concepts.
- The semantics of the extensions does not reflect an holistic approach to IAS. None of the extensions allows the representation of security countermeasures of all four types (legal, human-oriented, organisational and technical) which are distinguished in the RMIAS.

- Little attention is paid to the syntax of the extensions. As a result, the extensions lack cognitive effectiveness. The graphical elements of the extensions (if used at all as opposed to textual annotations) are often developed guided by intuition, rather than scientific principles. The papers, where the scientific principles are said to be followed, discuss the syntax at a very superficial level confirming that research regarding the design of cognitively effective security modelling notations is still in its infancy.

- The absence of the detailed evaluation of the syntax, semantics and overall effectiveness of the extensions examined. The evaluation is often limited to presenting a security-annotated BPMN diagram. In other cases the possibility of transforming security-annotations into executable configurations is evaluated. No evaluation of the cognitive effectiveness of the syntax or the ontological completeness of the semantics or the overall effectiveness of the extensions was found in the examined papers.

The next chapter introduces Secure*BPMN which attempts to address the above listed shortages of the analysed extensions. At the end of Chapter 7 in Section 7.5, after Secure*BPMN and its evaluation are described, the bullet points listed above are revisited and it is explained how Secure*BPMN deals with these issues.

Chapter 6

Secure*BPMN

This chapter introduces Secure*BPMN, a technique enabling security-annotation of business process models expressed in BPMN[1]. The literature analysis contained in the previous section reveals some drawbacks of the existing security extensions which Secure*BPMN attempts to remedy. This chapter elaborates on the semantics and syntax of Secure*BPMN. The BPMN metamodel is extended with the security concepts extracted from the RMIAS. The visual vocabulary and compositional rules of Secure*BPMN are introduced. This chapter also outlines the annotation procedure, which should be followed when using Secure*BPMN, and gives an illustrative annotation example. The Secure*BPMN stencils for Microsoft Visio and OmniGraffle are presented.

6.1 Secure*BPMN semantics

The semantics of Secure*BPMN is based on the RMIAS. The reasons for choosing the RMIAS as the basis for the semantics of Secure*BPMN are summarised below:

1. The RMIAS is intended to enhance communication and for educational purposes. It is suitable for a wide audience with a range of backgrounds.

2. The RMIAS approaches IAS holistically and not as a purely technical issue. An information system, in the context of the RMIAS, is understood to be a complex socio-technical phenomenon and is not limited to the IT components.

[1]For the purpose of this thesis, it is assumed that a business process model, which is to be annotated with security details, is correct from the business viewpoint, structurally sound (i.e. it has one start event, one end event and each node is on a path from the start event to the end event [9]) and optimised. The improvement and optimisation of business processes regarding aspects other than security is out of the scope of this research.

3. The qualities of the RMIAS as a conceptual model are analytically and empirically evaluated in a multiphase process. The evaluation confirms that the RMIAS is an adequate representation of the IAS domain suitable for experts independent of the level of their expertise in IAS and technical knowledge.

4. The RMIAS captures the concepts that are fundamental to the IAS domain. The evaluation confirms that the RMIAS is a complete and accurate representation of IAS.

Overall, among other attempts to represent the IAS knowledge, which are analysed in Chapter 2, the RMIAS is better aligned with the intended purpose of Secure*BPMN as it is described in Section 1.2.

Since it was previously demonstrated that the constructs of the RMIAS could not be effectively represented using the existing BPMN elements (Section 5.3.4), this chapter extends BPMN for IAS modelling.

In order to extend the BPMN metamodel (1) a set of security concepts is derived from the RMIAS and (2) the BPMN metamodel is extended with these security concepts as described below.

6.1.1 Extraction of security concepts from the RMIAS

Among the four dimensions of the RMIAS, the security development life cycle dimension is a timeline along which the concepts of the other three dimensions exist. Business process models, which are to be annotated using Secure*BPMN, are developed at the first stage of the life cycle - security requirements engineering - and may be further adjusted at the stage of security design. Thus, in business process models the ontological security concepts of three dimensions of the RMIAS, namely the Information Taxonomy, Security Goals and Security Countermeasures dimensions, should be represented.

The following security concepts are identified in the above three dimensions of the RMIAS:

- Information (Information Taxonomy Dimension),
- Information Sensitivity (Information Taxonomy Dimension),
- Information Form (Information Taxonomy Dimension),
- Information State (Information Taxonomy Dimension),

- Information Location (Information Taxonomy Dimension),
- Security Goal (Security Goals Dimension),
- Security Goal Criticality (Security Goals Dimension),
- Security Goal Name (Security Goals Dimension),
- Security Countermeasure (Security Countermeasures Dimension)
- Security Countermeasure Type (Security Countermeasures Dimension),
- Security Countermeasure Description (Security Countermeasures Dimension), and
- Security Association (arrows depicting the logical interdependences between the dimensions).

These security concepts are incorporated into the BPMN metamodel as security classes (Section 6.1.2).

It is also necessary to introduce into the extended BPMN metamodel the classes, which are not explicit in the RMIAS, but help to show the relationships between the existing classes of the BPMN metamodel and security classes. The following additional security classes are identified:

- Secure Swimlane,
- Secure Swimlane Location, and
- Access Permission.

Table 6.1 lists the classes derived from the RMIAS concepts (Figure 3.1) as well as the additional security-related classes, which are to be added to the BPMN metamodel. Table 6.1 also explains the reasons for the incorporation of each concept into the BPMN metamodel.

Table 6.1: Security concepts to be introduced into the BPMN metamodel

Security Concept Name	**Reason for the incorporation into the BPMN metamodel**
Information/ Secure Data	In the RMIAS, characteristics such as location, state, form and sensitivity are indicated for a specific piece of information. In BPMN, information is represented by the elements of category Data such as Data Object and Data Store. Information may also be represented by the element Message. A BPMN element of the category Data, which is enriched with such security attributes as location, state, form and sensitivity, is referred to as a Secure Data.
Information Sensitivity	Derived from the RMIAS, Information Taxonomy Dimension. Indicates the sensitivity of the BPMN elements of the category Data (i.e. Data Object, Data Store) and the BPMN element Message.
Information Form	Derived from the RMIAS, Information Taxonomy Dimension. Indicates the form of the BPMN elements of the category Data (i.e. Data Object, Data Store) and the BPMN element Message.
Information State	Derived from the RMIAS, Information Taxonomy Dimension. Indicates the state of the BPMN elements of the category Data (i.e. Data Object, Data Store) and the BPMN element Message.
Information Location	Derived from the RMIAS, Information Taxonomy Dimension. Indicates the location of the BPMN elements of the category Data (i.e. Data Object, Data Store) and the BPMN element Message.
Security Goal	Derived from the RMIAS, Security Goals Dimension. Indicates the security issues which may arise in a business process and specifies security goals that must be achieved within the process.
Security Goal Name	Derived from the RMIAS, Security Goals Dimension. Specifies which of the eight goals of the IAS-octave is important for an organisation in the context of a specific process.
Security Goal Criticality	Derived from the RMIAS, Security Goals Dimension and the right arrow which depicts the interconnection between the Information Taxonomy and Security Goals Dimensions. States the need for prioritising security goals. Indicates how critical a security goal is for an organisation in the settings of a specific process.
Security Countermeasure	Derived from the RMIAS, Security Countermeasures Dimension. Helps to show techniques and activities that shall be implemented/undertaken within a process in order to mitigate risks to information and achieve outlined security goals.

Continued on the next page

Table 6.1 – *Continued from the previous page*

Security Concept Name	**Reason for the incorporation into the BPMN metamodel**
Security Countermeasure Type	Derived from the RMIAS, Security Countermeasures Dimension. Indicates the type of a security countermeasure.
Security Countermeasure Description	Derived from the RMIAS, Security Countermeasures Dimension. Provides a detailed description of a security countermeasure.
Secure Swimlane	Not explicit in the RMIAS. However, a link between business process concepts and security concepts is required. This link in Secure*BPMN is drawn using the BPMN class Swimlane. In a security-annotated BPMN diagram, a Swimlane represents a participant of a process (e.g. a user, a department or an organisation). In a process it is required to specify security attributes for each participant (e.g. to the documents of which levels of sensitivity a participant has access and the location of a participant). A Swimlane BPMN element enriched with security attributes is referred to as a Secure Swimlane.
Secure Swimlane Location	Derived from the RMIAS, Information Taxonomy Dimension. In the RMIAS, the location is one of the characteristics of information. The location of a Swimlane has the same meaning as the location attribute of information in the RMIAS. The link of the class Location and the class Secure Swimlane is guided by the fact that in a process model the location of all Data elements within one Pool/Lane is the same as the location characteristic of a Swimlane. Thus, specifying the location of a participant removes a need to specify the location attribute for each Data element the participant deals with. The location attribute of a Swimlane reflects how much control the organisation-annotator has over information within the Swimlane.
Access Permissions	Not explicit in the RMIAS, but draws a link between a business process concept participant (depicted by a Swimlane in BPMN) and a security concept sensitivity. Access permission indicates whether a participant has access to the documents of a certain level of sensitivity.

Continued on the next page

Table 6.1 – *Continued from the previous page*

Security Concept Name	**Reason for the incorporation into the BPMN metamodel**
Security Association	In the RMIAS, it is illustrated as the interrelationship between the dimensions. For example, the RMIAS assumes that a security goal is specified for a specific piece of information depending on its security characteristics, while a security countermeasure mitigates a certain security goal. In a security-annotated diagram Security Connecting Object helps to link security classes with BPMN classes and with other security classes.

6.1.2 Extended metamodel

Figure 6.1 depicts the BPMN metamodel extended with the security concepts identified in the previous section. The unshaded classes belong to the BPMN metamodel, as discussed in Section 5.3.3. The security-related classes, added to the metamodel, are shaded.

Figure 6.1 is not intended to illustrate the interrelationship between the existing BPMN classes and security constructs, but shows a range of modelling objects (classes) required for the design of a secure business process.

Figure 6.2 provides the clarification of some parts of the extended metamodel. Further in this section, the extended metamodel is explained. The definitions of the security concepts extracted from the RMIAS are adopted as described in the RMIAS in Chapter 3 and, therefore, are not reiterated in this section.

In Figure 6.1, the class Secure Business Process Diagram is a specialised form of the base class Business Process Diagram.

The class Security Goal is associated with the class Criticality (Figure 6.2a). In the context of this thesis, the instances of the class Criticality may adopt values such as Low, Medium and High. The reasons for choosing this set of values to classify the criticality of a security goal are discussed in Section 3.6. Each instance of the class Security Goal may have zero (criticality has not been set) or one instance of the class Criticality associated with it.

The class Security Goal is also associated with the class Name. The class Name may adopt its value from the IAS-octave, i.e. may be Confidentiality, Integrity, Availability, Authenticity & Trustworthiness, Non-repudiation, Accountability, Auditability and Privacy.

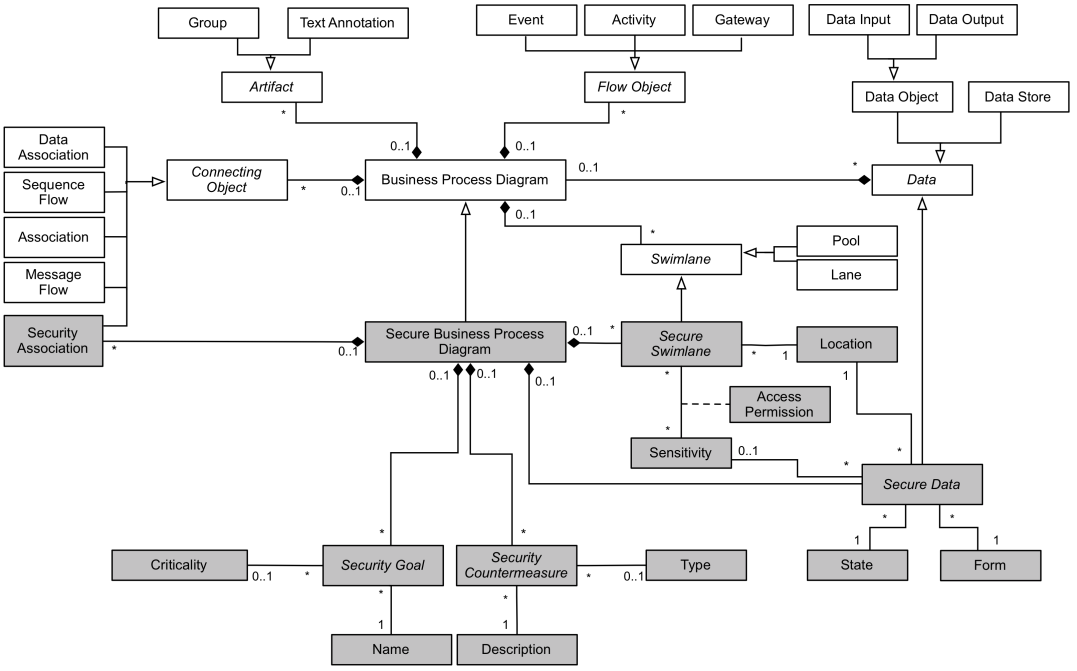


Figure 6.1: The BPMN metamodel extended with security elements

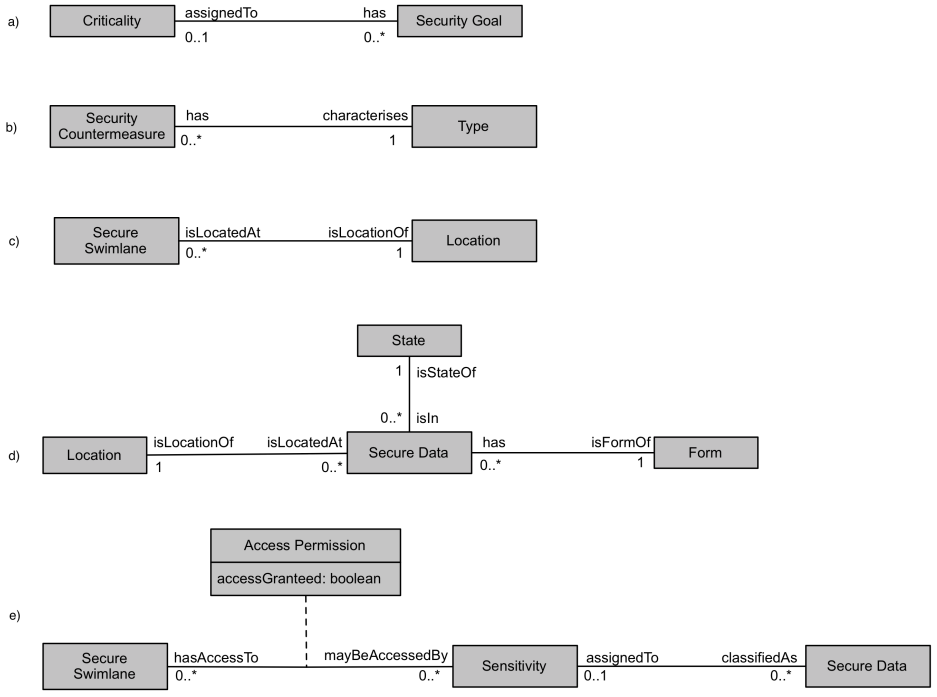


Figure 6.2: The clarification of the extended BPD metamodel

Each instance of the class Security Countermeasure is associated with only one instance of the class Type (Figure 6.2b). Four types of security countermeasures, which are distinguished in the RMIAS, are adopted by Secure*BPMN: organisational, technical, human-oriented and legal.

Each instance of the class Secure Data is associated with only one instance of the classes State, Form, Sensitivity and Location. It means that an instance of the class Secure Data Object or Secure Data Store may have only one form and the level of sensitivity, be in one state, and be positioned only at one Location (Figure 6.2d-e).

The Swimlane BPMN element may be used for different purposes [160]. In the proposed approach, it is assumed that a Swimlane (e.g. a Pool/Lane BPMN element) depicts an organisation, a department of an organisation or an individual. With this connotation in mind, the class Secure Swimlane may be associated with the class Sensitivity. The association between the classes Secure Swimlane and Sensitivity contains information on whether an individual, department or organisation depicted by the Swimlane has access to the information of that specific level of sensitivity (Figure 6.2e). Therefore, an association class Access Permission is attached, with a dotted line, to the primary association between the classes Secure Swimlane and Sensitivity.

Any instance of the class Secure Swimlane may be associated with only one Location (Figure 6.2c). BPMN does not provide the default functionality for depicting a location [13]. Secure*BPMN introduces a rule that if within one process the same participant undertakes activities at different locations, then each location shall be depicted by a separate Lane or Pool, where appropriate, and the location attribute shall be set for each Pool/Lane.

6.2 Secure*BPMN syntax

6.2.1 Importance of a Syntax

In order to facilitate communication among experts with different backgrounds and enhance the visibility and transparency of security issues in a business process, Secure*BPMN has to be cognitively effective. Cognitive effectiveness refers to the speed, ease and accuracy of the processing of a notation by people [31].

A graphical visualisation of security constructs is a way to improve their cognitive effectiveness. The decision to develop a graphical security modelling language for the purpose of this thesis is

guided by the following facts [30, 31]:

1. Graphical representations are specifically designed to be processed by people and with the main purpose to enhance communication and problem solving;
2. Diagrams, in general, surpass natural languages in presenting information in a concise and precise form, and in time for which the information is remembered;
3. Graphical annotations are more easily comprehensible, particularly by non-technical experts and novices, than text-based annotations; and
4. The cognitive effectiveness of a visual notation may be empirically evaluated.

Moody [30] discusses in greater detail the advantages of graphical representation. He also notes that, although syntax is not less important than semantics, it is often neglected by the developers of new visual notations[2]. The possible reasons for the scant attention to the syntax of modelling languages are (1) the assumption of the early researchers of the IS design methods, who most likely had a mathematical background, that only semantics may be rigorously analysed; (2) the immaturity of the methods for the analysis of the effectiveness of visual representation; and (3) the misconception of syntax as a trivial aesthetic issue which is irrelevant to the overall effectiveness of a notation [30].

Refuting the insignificance of the syntax of a modelling language, research findings show that form (syntax) has, at least, equal or even greater effect on cognitive effectiveness than content (semantics). Comprehension and, as a result, problem solving abilities, may be significantly influenced by the minor changes of the visual representation of a problem [30]. As confirmed by empirical studies, the understanding of novices in particular is strongly affected by the effectiveness of a syntax [30].

Echoing the statement about the lack of attention to syntax, the previous chapter demonstrated that the design rationale for the graphical security-annotations in the related works is either not documented or it is only addressed at a superficial level, and the choice of symbols is often guided by pure intuition and common sense. The lack of a theoretical foundation supporting the syntax design (an unselfconscious design culture) may often lead to counter-intuitive solutions and to the missed possibilities in the design space, to the inclusion and propagation of imperfect design solutions [30].

[2]The structure of a modelling notation is described in Appendix A.2

However, not every graphical notation is cognitively effective and, therefore, superior in its cognitive power to a textual notation. Cognitive effectiveness must be designed into a notation by strict adherence to the theories and empirical evidence related to the cognitive effectiveness of modelling notations [30].

6.2.2 Guidance for the Secure*BPMN Syntax Design

The design of the Secure*BPMN syntax is stipulated by the scientific facts synthesised in the "Physics" of Notations - the Theory for Visual Notation Design (TVND) [30], which outlines nine principles for optimising the cognitive effectiveness of a modelling notation. The detailed description of the TVND along with the justification of its choice as the theoretical basis for the design of the Secure*BPMN syntax are presented in Section 7.2.2.1.

The following section outlines the shapes and icons of Secure*BPMN, and the way they were elaborated. For consistency, the detailed analytical analysis of the cognitive effectiveness of Secure*BPMN and the discussion about how the syntax of Secure*BPMN satisfies the principles of the TVND are contained in Section 7.2.2 where the evaluation of Secure*BPMN using other frameworks is also presented. The discussion of the trade-offs between the principles of the TVND which were made while designing the Secure*BPMN syntax are also given in Section 7.2.2. The empirical evaluation of the cognitive effectiveness of Secure*BPMN was conducted as a part of the experiments testing the pragmatic value of Secure*BPMN and is described in Section 7.3.

The syntax of Secure*BPMN satisfies the requirements towards extensions which are declared in the BPMN standard ISO/IEC 19510:2013(E) and encapsulated in Section 5.3.5.

6.2.3 Secure*BPMN Visual Vocabulary

6.2.3.1 Security Goal

A **security goal** is depicted with a circle-based shape, derived from a target symbol (Figure 6.3a).

A circle is used in BPMN to represent an Event. To avoid confusion between an event symbol and a security goal symbol, the size of a security goal symbol in a business process model should be

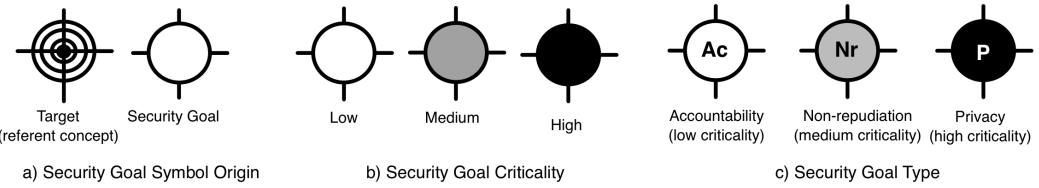


Figure 6.3: Secure*BPMN Visual Vocabulary. Security Goals.

1.5-2 times larger than the size of an Event symbol. The darkness[3] of a security goal symbol is used to visualise the **criticality** of a security goal (Figure 6.3b):

- Low Criticality - low darkness;
- Medium Criticality - medium darkness; and
- High Criticality - high darkness.

The **name** of a security goal is marked by the corresponding initial letter(s) placed in the middle of a security goal symbol (Figure 6.3c): Confidentiality (C), Integrity (I), Availability (A), Authenticity & Trustworthiness (AT), Non-repudiation (Nr), Accountability (Ac), Auditability (Au) and Privacy (P).

6.2.3.2 Security Countermeasure

A **security countermeasure** is depicted with a padlock symbol (Figure 6.4a). The **type** of security countermeasure is visualised with a semantically transparent icon inside a padlock (Figure 6.4b). A padlock symbol is accompanied by a detailed text **description** of a security countermeasure (Figure 6.4c). Figure 6.4c shows, as an example, the legal security countermeasure "Non-disclosure Agreement" as it must appear in an annotated model.

The following approach was followed to derive the icons indicating the type of a security countermeasure:

[3] In the TVND [30] this visual variable is referred to as brightness. It defines a scale of relative brightness or darkness. In this work to coincide with *low-medium-high* categorisation of security goals, it is logical to refer to it as darkness so that a *highly* critical security goal is depicted using a symbol with *high* darkness.

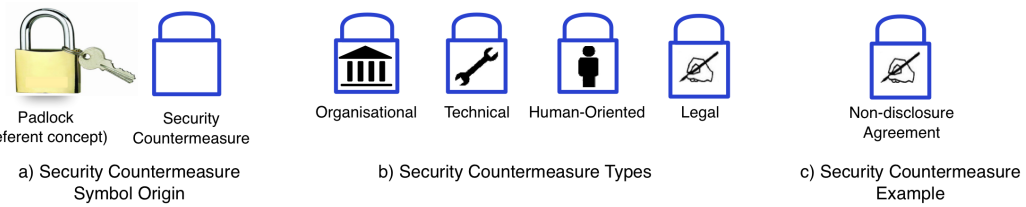


Figure 6.4: Secure*BPMN Visual Vocabulary. Security Countermeasures.

First step - a search on a Google Search Engine was performed using the name of a security countermeasure type as a keyword;

Second step - among a large number of the returned images, two or three images were selected for each type of a security countermeasure. An image was selected if (1) it is not in use in BPMN, (2) it may be presented in the form which maintains the BPMN feel-and-look and (3) it may be reasonably easy drawn by hand; and

Third step - out of the samples for each type of a security countermeasure chosen at the second step a final icon was selected that better complies with the connotation of a keyword in Secure*BPMN.

A set of symbols selected at the second step for a technical security countermeasure included a gear (Figure6.5a) and a spanner (Figure6.5b). The gear(s) icon is in use in BPMN and indicates a service task. Hence, the final preference was given to a spanner.

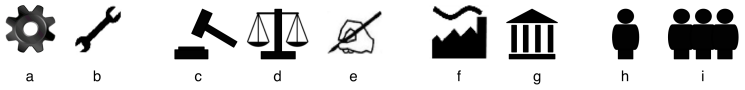


Figure 6.5: The sample of icons to indicate types of security countermeasures

A sample for a legal security countermeasure included the following symbols: the hammer of justice (Figure6.5c), the scales held by Lady Justice (Figure6.5d) and a hand signing a contract (Figure6.5e). The first two, although being associated with the term "legal" have the connotation to justice as moral rightness and fairness. The last of the three is more adequate for denoting a legal security countermeasure. In Secure*BPMN, a legal security countermeasure refers to a legal agreement, rather than justice in its general sense.

A sample for an organisational security countermeasure included two icons: a factory with chimney (Figure6.5f) and an official building (Figure6.5g). The icon of an official building is in use to

refer to an organisation in the empirically evaluated icon-based labelling scheme known as Protective Commons developed for the user-friendly communication of security needs and controls at inter-organisational level [190]. Hence, the final preference was given to the official building icon.

For a human-oriented countermeasure, the sample of icons consisted of a single human figure icon (Figure6.5h) and a group of people icon (Figure6.5i). The icons are relatively small in an annotated digram. Due to the facts that a single human figure is better distinguishable in a small format and it is easier to be drawn by hand than a group of people icon, the final preference was given to the single human figure icon.

In coloured models, the recommended colour of a security countermeasure symbol is blue, following the sign for mandatory actions in ISO 7010:2011(E), M001 - *Graphical symbols. Safety colours and safety signs. Registered safety signs*. To ensure that a security-annotated business model retains information while being displayed in a black-and-white format and is suitable for colour-blind users, colour in Secure*BPMN is used in a redundant way.

A security countermeasure symbol (excluding the description) must have the same height as a diameter of a security goal symbol.

6.2.3.3 Information Sensitivity

To visualise such characteristics of information as **sensitivity** and **form** in a business process model, markers are applied to Data Object, Message and Data Store BPMN elements.

In order to derive the markers for information sensitivity[4], the Traffic Light Protocol information sensitivity classification and colour-enhanced labelling scheme [108, 111] was taken as the basis. This scheme is introduced in Section 3.5.2.

A circle filled with a colour with none or up to three exclamation marks placed in the middle is used in the Traffic Light Protocol scheme [108] to label the information of the various levels of sensitivity (column 1 of Table 6.2). Since a circle is in use in BPMN and represents an Event, Secure*BPMN cannot adopt the Traffic Light Protocol labelling scheme as it is presented in [108]. The circle shape of the Traffic Light Protocol labels (column 1 of Table 6.2) is replaced in Secure*BPMN with a pentagon shape (column 4 of Table 6.2). The colour of the symbols is used in a redundant way as it is accompanied by the appropriate number of exclamation marks.

[4]The sensitivity of information is discussed in Section 3.5.2.

Table 6.2: Information Classification and Access Permissions Notations

1. Traffic Light Proposal labels	2. Colour	3. Traffic Light Proposal Classification	4. Secure*BPMN Sensitivity and Access Permission markers	5. Translate Classification Schema
	Red	Highly Sensitive		Confidential
	Amber	Sensitive		Restricted Sharing
	Green	Normal Business		Proprietary
	White	Public		Public

Secure*BPMN sensitivity markers may be applied to depict different classification schemes. Secure*BPMN does not adopt the Traffic Light Protocol scheme as it is outlined in [108] and reproduced in the column 3 of Table 6.2. The Traffic Light Protocol was only used to derive the markers.

As a sample classification scheme in the annotation examples further in this section, and in the illustrative example in Section 6.4, the classification scheme of Translate[5] is exploited. Translate classifies its information as follows:

- *Public*: press releases, advertisement emails and brochures, and invitations to tender;
- *Proprietary*: original customers' documents, translated documents in paper or electronic form;
- *Restricted Sharing*: financial statements;
- *Confidential*: salaries, financial reports, audit opinion & reports, tender bids.

Columns 4 and 5 of Table 6.2 show the correspondence between the Secure*BPMN sensitivity markers and the levels of classification adopted by Translate.

The sensitivity of a Data Object, Message and Data Store is depicted by placing a corresponding sensitivity marker at the bottom right corner of the element (Figure 6.6).

[5]Translate is introduced in Section 3.5.2. The description of Translate is outlined in Appendix A.5.

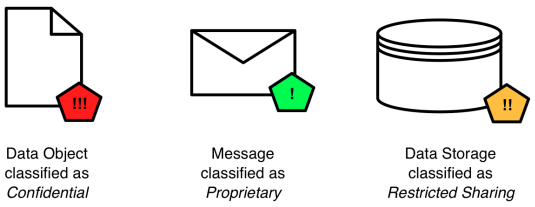


Figure 6.6: Secure*BPMN visual vocabulary. Application of sensitivity markers.

6.2.3.4 Information Form

To depict the **form**[6] of a Data Object the set of semantically transparent icons is used (Figure 6.7a). The form markers are placed at the top right corner of Data Object, Message and Data Store BPMN elements as depicted in Figure 6.7b.

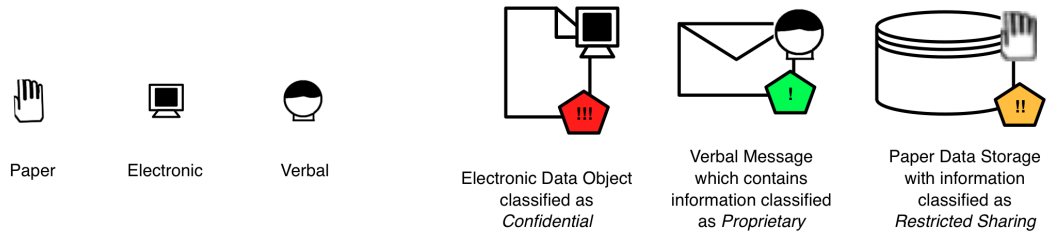


Figure 6.7: Secure*BPMN Visual Vocabulary. Form markers and their application.

6.2.3.5 Information and Secure Swimlane Location

The BPMN specification acknowledges that each model which shows a collaborative business process involving more than one participant may be observed from several different points of view. A reader may observe the diagram from the perspective of one participant or another. The BPMN documentation does not allow the specification of the viewpoint adopted [160, Sec. 7.1.1].

The viewpoint from which the diagram is observed is an important aspect in Secure*BPMN, because security-annotations are conducted from the perspective of the participant whose viewpoint is adopted. Further, in the text the participant, whose viewpoint is adopted, is referred to as an annotator. The location attribute of a participant and, consequently, the information[7] he/she pos-

[6]The form of information is discussed in Section 3.5.1.

[7]The location of information is discussed in Section 3.5.3.

sesses, depends on the point of view adopted by the annotator. It means that the diagram is annotated according to the information classification scheme of the annotator and with the purpose of protecting the information of the annotator or the information for which the annotator is responsible due to contractual agreements. The security goals are also set from the perspective of the annotator. To avoid confusion, in all further annotated examples security-annotation is conducted from the perspective of Translate.

A participant is presented in BPMN by a Swimlane (Pool or Lane) element. The location attribute of a Swimlane representing an annotator is set as *controlled*, because the organisation controls information while it is within this Swimlane and may implement the required security countermeasures at its discretion. A Swimlane representing a customer may be labelled as *uncontrolled*, since an annotator cannot control information while it is processed or stored by a customer. A Swimlane of a cloud-provider, may be designated as a *partially controlled* environment: on the one hand information is out of physical control of an annotator, but on the other hand an annotator may change information storage and processing settings. The location markers are textual markers (Figure 6.8a) and must be placed within a Swimlane area beneath the Swimlane name (Figure 6.8b).

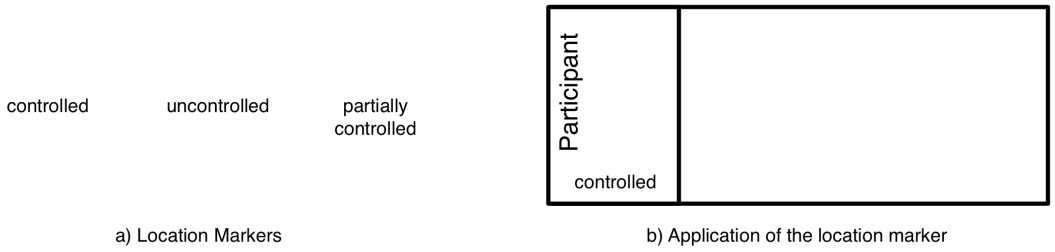


Figure 6.8: Secure*BPMN Visual Vocabulary. Location markers and their application..

The location attribute of a Data Object, Message or Data Store is not depicted by a specific marker, but is identified based on the position of an object in a model. For example, if a Data Object is placed within a Pool designated as an *uncontrolled* environment then the location attribute of the Data Object is also *uncontrolled*.

BPMN does not allow the indication of the location of an activity by default [13]. Secure*BPMN imposes the rule so that each different location of the same participant must be depicted by a separate Swimlane. The location attribute must be set for each Swimlane.

6.2.3.6 Access Permission

Access permissions of a participant are depicted by placing access permission (sensitivity) markers (column 5 of Table 6.2) on the right of the Swimlane name (Figure 6.9). The presence of the marker means that the Participant depicted by this Swimlane has access to the information of the level of sensitivity to which the marker corresponds.

Figure 6.9a indicates that Translate has access to the documents of all four levels of sensitivity (i.e. *Public*, *Proprietary*, *Restricted Sharing* and *Confidential*).

Figure 6.9b depicts a pool of Translate's customer. The access permission marker within this pool indicates that a customer is only granted access to the information which is classified by Translate as *Public*. A customer must not access information of any other level of sensitivity.

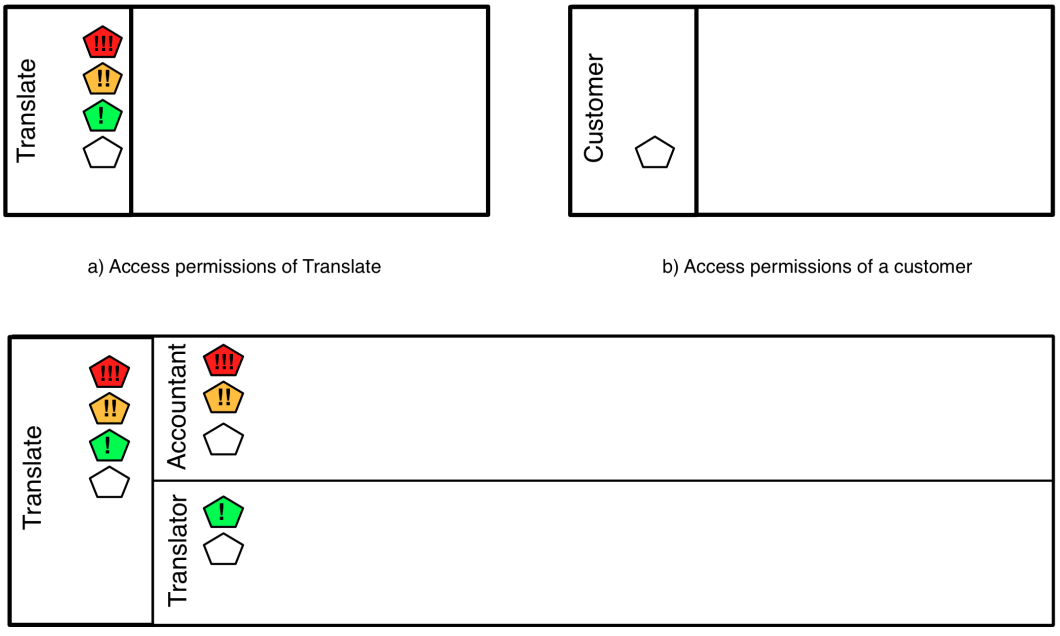


Figure 6.9: Secure*BPMN Visual Vocabulary. Indication of access permissions.

Although Translate as a company has access to the information of any level of sensitivity, the access permissions for different roles within a company vary. Figure 6.9c shows that the accountant of Translate is granted access to the information classified as *Confidential*, *Restricted Sharing* and *Public* (i.e. financial statements, reports etc.). However, the accountant does not have right to access *Proprietary* information (i.e. the documents submitted for translation). Figure 6.9c also

shows that a translator of the company, who deals with customers' documents directly, is granted access to the documents classified as *Proprietary*, while must not access the documents classified as *Confidential* or *Restricted Sharing*.

The access permission markers denote the permitted direction of data flow. Thus, data must not be sent to a Participant who has no access to the level of classification this data has. More detailed example of this is provided in Section 6.4.

6.2.3.7 Information State

The **state**[8] attribute of the elements of the category Data does not require an explicit visual representation, because the syntax of BPMN is sufficient to address it. State may be defined based on the position of a element in a model according to the rules outlined in Table 6.3 and based on the name of an element to which a Data element is attached. The nature of an Activity or an Event, as it is specified in a model, normally provides sufficient information in order to identify the state of information during the activity or event. The introduction of a new visual construct in this case would cause symbol redundancy and increase language complexity which is not recommended by the TVND.

The state attribute is constant for the Message and Data Store elements and is as follows: Message - transmission[9]; Data Store - storage[10].

The state of a Data Object associated with a BPMN element Activity may adopt any of the five values depending on the description of the activity. For example, if the activity name is "Produce Bid" and there is a Data Object named Bid attached to it, it means that the state of a Bid during this activity is creation.

A Data Object associated with an Event may be in the state of creation, transmission, processing or destruction depending on the nature of the Event. A Data Object associated with Message Flow is in the state of transmission. A Data Object associated with Sequence Flow may be in the state of creation, transmission, processing or destruction depending on the nature of the element between which the sequence flow is drawn.

[8] The state of information is discussed in Section 3.5.4.

[9] In BPMN, the Message element reflects the content of communication and is depicted over message flow (Table 5.1).

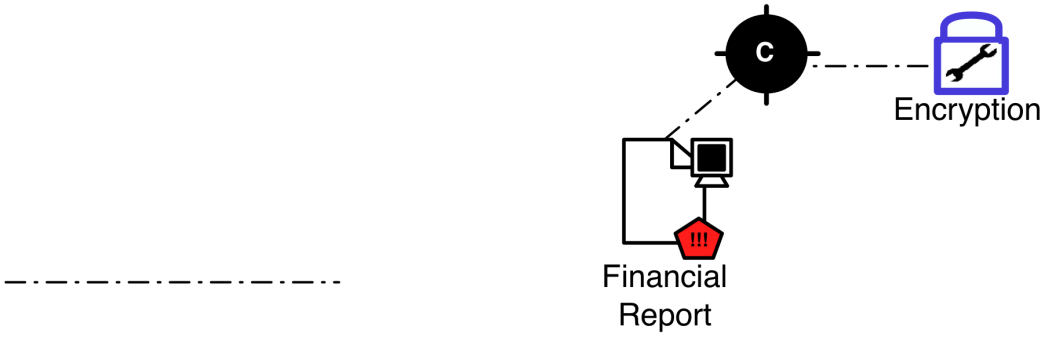
[10] In BPMN, Data Store depicts a stored information that persists beyond the scope of the process [161, p.207]

Table 6.3: The state of information by position in a model

	Information State				
BPMN basic element	Creation	Transmission	Storage	Processing	Destruction
Data Object	X	X	X	X	X
Data Store			X		
Message		X			
Activity	X	X	X	X	X
Event	X	X		X	X
Message Flow		X			
Sequence Flow	X	X		X	X

6.2.3.8 Security Association

Security association is depicted by a dash-dot line which is shown in Figure 6.10a. It depicts the association between a security goal and a BPMN element or between a security goal and a security countermeasure.



a) Security association line

b) Use of the security association line

Figure 6.10: Secure*BPMN Visual Vocabulary. Security association line and its application..

Figure 6.10b shows how a security association line may be used. In this example, the security goal *confidentiality* is associated with the *Confidential* electronic document Financial Report. This association means that Translate is concerned with the confidentiality of the Financial Report. Here, the association line depicts the link between a technical security countermeasure *encryption* and the security goal *confidentiality* indicating that the goal may be achieved by means of this security countermeasure.

6.2.4 Secure*BPMN Visual Grammar

The Secure*BPMN compositional rules are presented in Table 6.4, where the following abbreviations are used:

- X - association is possible and must be depicted using a security association line;
- M - attribute is depicted in a model by a marker;
- P - attribute is identified by a position of an element in a model; and
- C - constant parameter (Section 6.2.3.7).

Strict compositional rules may lead to the reduced correctness and clarity of an annotated diagram [165]. Table 6.4 shows that the Secure*BPMN compositional rules are flexible. For example, a security goal and security countermeasure may be associated with any BPMN element.

Table 6.4: Secure*BPMN Compositional Rules

	Security Objects		Security Attributes						
	Security Goal	Security Countermeasure	Sensitivity	Form	Location	State	Access Permissions	Type/Name	Criticality
BPMN basic element									
Pool/Lane	X	X			M		M		
Data Object	X	X	M	M	P	P			
Message/DataStore	X	X	M	M	P	C			
Group	X	X			M				
Secure*BPMN elements									
Security Goal		X						M	M
Security Countermeasure	X							M	

6.3 Secure*BPMN Recommended Annotation Procedure

This section describes how security-annotation of a business process model should be conducted. This procedure is intended to ensure that all security elements are addressed.

The annotation procedure provides only a general guidance. Secure*BPMN visual vocabulary may be applied in a different sequence and in the combination which better suits the needs of an annotator. There may be situations when a smaller set of Secure*BPMN constructs would be

sufficient in order to facilitate a discussion in some groups (e.g. a team may avoid setting access permissions and documents' attributes, and concentrate only on security goals or only on security countermeasures). In such cases some steps of the annotation procedure may be skipped.

The recommended security-annotation procedure consists of five steps which are described in Table 6.5.

Table 6.5: Secure*BPMN Recommended Annotation Procedure

Step 1: Set the location attribute for each Pool/Lane *Annotator(s)*: Business Expert[11] *Description*: A business expert specifies the location attribute for each participant (Swimlane) in a diagram. The location attribute is set according to the level of control the organisation-annotator has over information in each Swimlane and using the scale *(controlled) - (partially controlled) -(uncontrolled)*. A business expert places the appropriate textual location markers underneath the Swimlane name *Relevant Secure*BPMN elements*: textual location markers
Step 2: Specify access permissions for each participant *Annotator(s)*: Business Expert *Description*: A business expert possesses information about who shall/shall access documents of the different levels of sensitivity. For each participant of a process, a business expert specifies access permissions by placing the access permission (sensitivity) markers, which correspond to the sensitivity levels to which a participant is granted access, in the Swimlane which illustrates the participant. *Relevant Secure*BPMN elements*: access permissions (sensitivity) markers
Step 3: Specify the form and sensitivity attribute for each Data element *Annotator(s)*: Business Expert *Description*: A business expert sets the form and sensitivity attributes for for each Data Object, Message and Data Store element in a diagram. This is done by placing a sensitivity marker at the bottom right corner and by placing a form marker at the top right corner of each Data element. *Relevant Secure*BPMN elements*: sensitivity markers and form markers

Continued on the next page

[11]It is assumed that a business expert possesses the detailed knowledge of a business process to be annotated. However, if this is not the case, a process participant or another expert who possesses such knowledge shall be involved in security-annotation. A business expert may conduct annotation either by himself/herself or with the assistance of a business process modeller who is familiar with Secure*BPMN.

Table 6.5 – *Continued from the previous page*

Annotation Step Description
Step 4: Identify and depict security goals *Annotator(s)*: Business Expert (with the involvement of other members of a multi-disciplinary team where help is required) *Description*: After all security settings of a business process are specified in the model during the previous three steps, a business expert may start to define security goals which must be achieved. A security goal may be set for any BPMN element. A business expert indicates the name and criticality of each goal. *Relevant Secure*BPMN elements*: security goal symbol
Step 5: Identify and depict security countermeasures *Annotator(s)*: Multi-disciplinary Team of Experts *Description*: After security goals are identified, the team starts a discussion on how the security goals specified at the previous step may be achieved, taking into account the security settings of a process. Each expert suggests security countermeasures within the scope of his/her knowledge and responsibilities. After the discussion, the security countermeasures which were approved by the team are depicted in the security-annotated diagram using a security countermeasure padlock symbol with the indication of the type of a countermeasure inside the symbol and the description of a countermeasure underneath the symbol. *Relevant Secure*BPMN elements*: security countermeasure symbol

6.4 Secure*BPMN illustrative example

In this example, the multidisciplinary team of Translate's employees, which includes a business owner (manager), legal adviser, system administrator and human-resources (HR) expert, is involved in the discussion and security-annotation[12].

[12]The annotation process as it is described in this section is based on two evaluation workshops with practitioners which took place on 6/11/2013 and 14/11/2013 (the details of the workshops are outlined in Section 7.3.2). The following participated in the workshops: software development and business analysts, records manager, who specialises in privacy legislation, data protection and information security officer, a manager of information security program, information systems security expert and cyber defence expert (Respondents 17-18 and 21-25 in Appendix A.11). The business process which is presented in this section was discussed by the participants of the workshops.

In this example, the security-annotation of a diagram is completed during one meeting. All members of the multi-disciplinary team are present at the meeting and they have at hand all the information which is needed to carry out security-annotation. In reality, the security-annotation of a business process diagram is not always a one-off process, but may be spread over a long period of time, depending on the complexity of a process, the availability of the members of a multi-disciplinary team and the knowledge of a process.

Beforehand the team received a presentation on the RMIAS to ensure that the experts have a harmonised understanding of the IAS concepts, and that security terminology is used coherently. The team also received a one hour training session on Secure*BPMN.

Figure 6.11 depicts a model of a financial audit process which is to be annotated with security details. At the end of the year, Translate sends financial statements to an external auditor by email, an independent firm engaged by Translate in order to express an opinion on whether the financial statements are free of mis-statements. On receipt of the financial statements, the auditor performs a substantive test of details (selects a sample of items from the account balances, and finds invoices and bank statements for those items). On completion, the auditor compiles a report and formulates an audit opinion and sends it to Translate by post. This process involves the sharing of sensitive information with an external organisation.

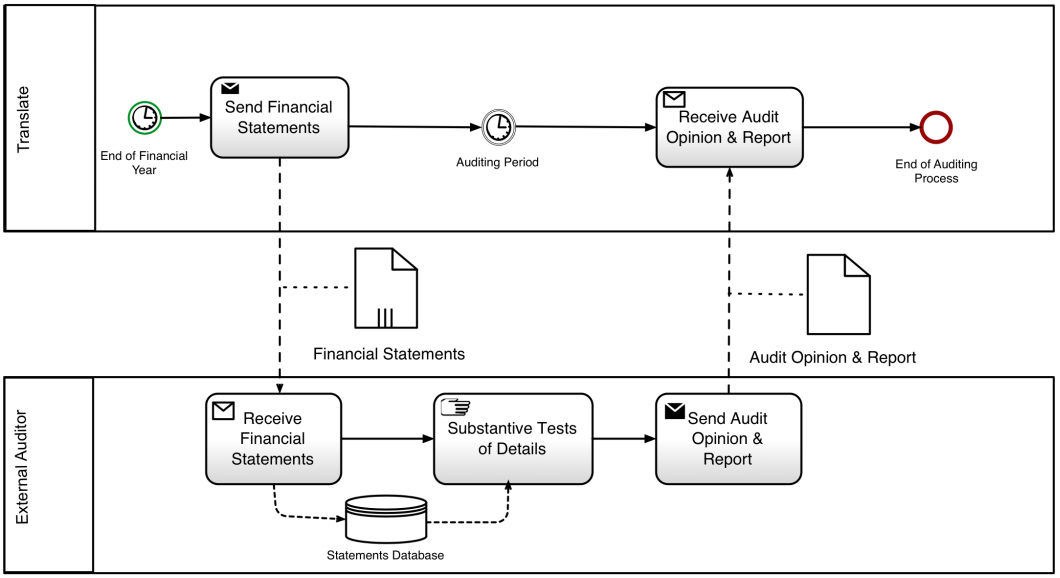


Figure 6.11: A financial audit business process

The security-annotation of the process is conducted in five steps following the procedure described in Table 6.5. The step-by-step security-annotation of the financial audit process is outlined below:

- *Step 1:* The manager (business expert) defines the viewpoint adopted for security-annotation: the annotations are to be made from the perspective of Translate. As a result, the pool of Translate in Figure 6.12 is marked as a *controlled* location (at the subsequent steps Translate's document classification scheme is used to mark the sensitivity of the documents and the security goals are also declared from the perspective of Translate). The external auditor is designated as a *partially controlled* location (Figure 6.12), because, although Translate may not physically control information after it is released to the auditor, there are contractual relationships between the auditor and Translate.

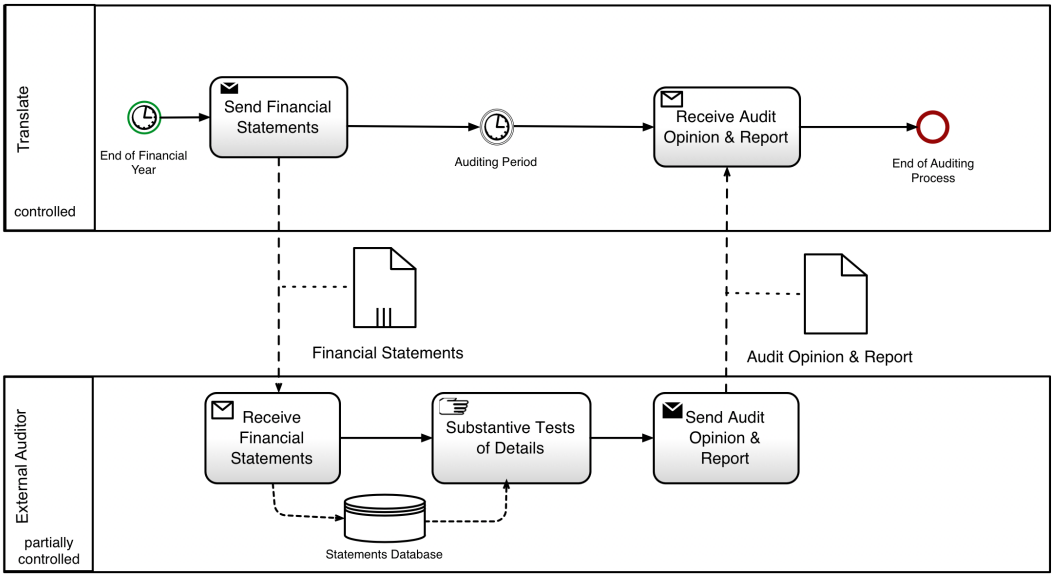


Figure 6.12: A financial audit business process model annotated with the location attributes.

- *Step 2:* The manager sets access permissions. Translate has access to information of all levels of sensitivity. The auditor has access only to the information classified by Translate as *Restricted Sharing* and *Public* (Figure 6.13).

- *Step 3:* The manager marks the form and sensitivity of each Data Object in the model. The financial statements are marked as electronic documents classified as *Restricted Sharing*, the audit report is marked as a *Confidential* paper document (Figure 6.14). This diagram also illustrates that, although according to the rules of Translate the auditor does not have access to the information classified as *Confidential*, the document the auditor produces for Translate must be classified as *Confidential* as soon as they are received by Translate. The access permission markers in this instance also denote the permitted direction of informa-

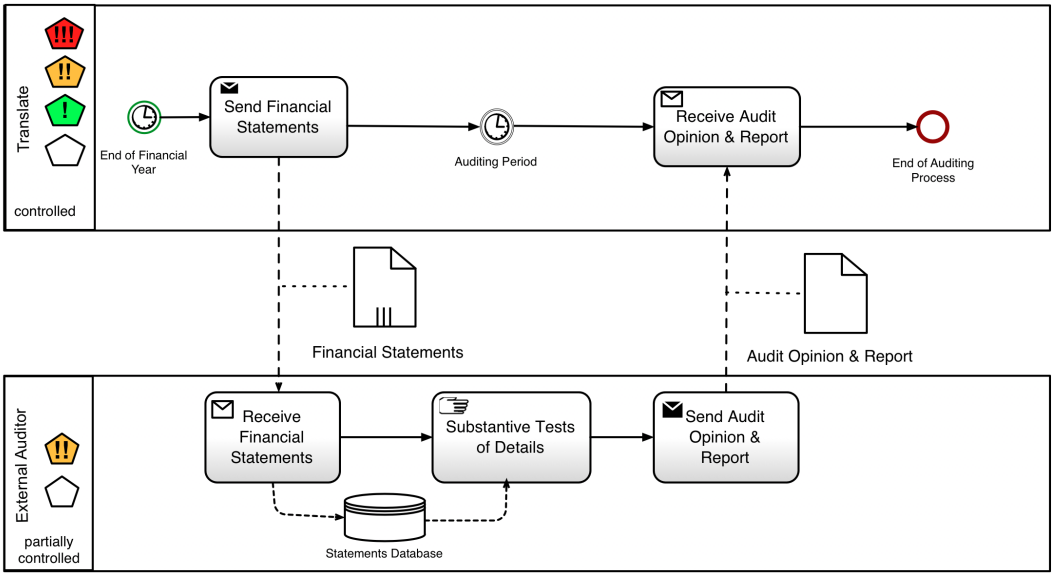


Figure 6.13: A financial audit business process model annotated with access permissions.

tion flow. In Figure 6.14, for example, a document classified as *Confidential* may move in the bottom-top direction, i.e. be transmitted from the auditor to Translate, but may not move in the top-bottom direction, i.e. be transmitted from Translate to the auditor.

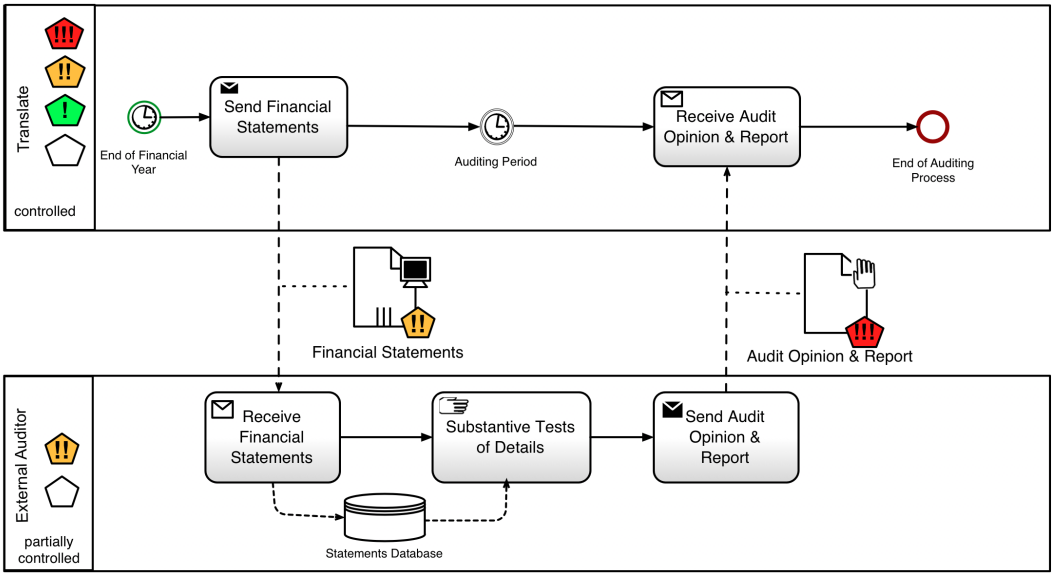


Figure 6.14: A financial audit business process model annotated with the information form and sensitivity attributes.

- *Step 4:* After all security settings of the process are depicted, the manager specifies security goals. The integrity of the financial statements is highly critical for Translate as well as the confidentiality of the audit report (Figure 6.15). Both security goal symbols are black-filled to indicate high criticality of the specified security goals.

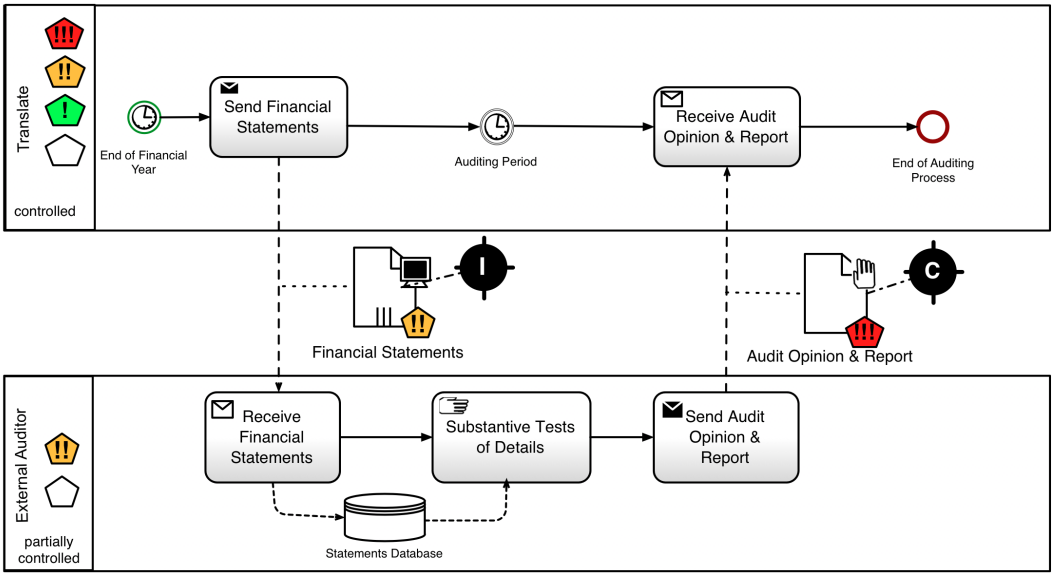


Figure 6.15: A financial audit business process model annotated with security goals

- *Step 5:* At this stage, the team familiarises itself with the details of the business process and the security-annotations rendered by the manager. The experts start the discussion of the security countermeasures which are required in order to achieve the specified security goals in the given business process.

  The system administrator recommends the encryption of the financial statements to ensure their integrity. The technical security countermeasure "Encryption" is added to the diagram (Figure 6.16). However, he explains that this technical countermeasure does not protect information while it is stored or processed by the auditor.

  To ensure the confidentiality of information while it is processed and stored by the auditor, the legal adviser suggests concluding a non-disclosure agreement with the auditor. The legal security countermeasure "Non-disclosure Agreement" is added to the diagram (Figure 6.16).

  The manager recommends two organisational countermeasures: to ensure that the audit report is labelled by the auditor according to Translate's classification scheme and that it

is sent by special delivery. Two organisational security countermeasures are depicted in Figure 6.16.

The HR expert recommends providing training on document classification for the staff of Translate to ensure that they deal with the documents according to their classification. The human-oriented security countermeasure "Training on document classification" is shown in Figure 6.16.

Finally, the team ensures that the countermeasures do not duplicate or impede each other.

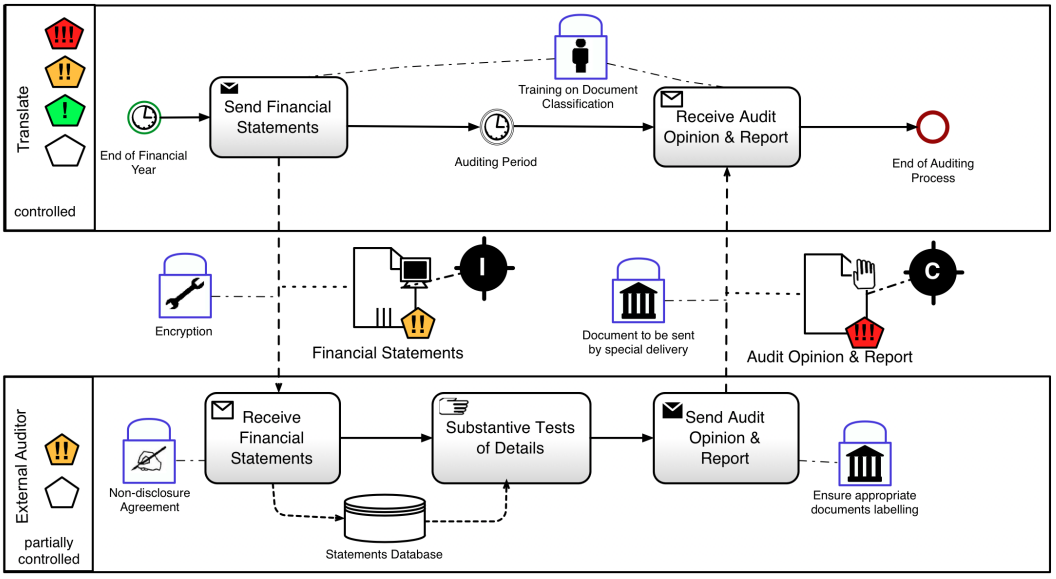


Figure 6.16: A financial audit business process model annotated with security countermeasures.

6.5 Secure*BPMN stencils

In order to assist with security-annotation, Secure*BPMN stencils were developed for two diagramming applications, Microsoft Visio Professional 2010 for Windows and OmniGraffle for Mac OS. The stencils may be used for the security-annotation of business process models in addition to any BPMN stencil for the diagramming applications named above.

OmniGraffle provides a graphical interface for the development of custom stencils. Using this functionality, the stencil was created containing the Secure*BPMN graphical vocabulary.

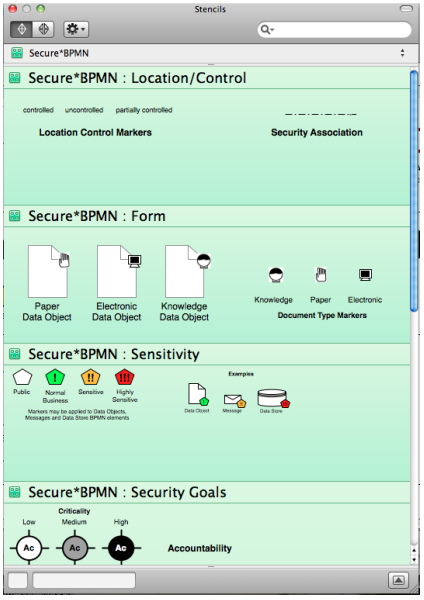


Figure 6.17: Secure*BPMN stencil for OmniGraffle

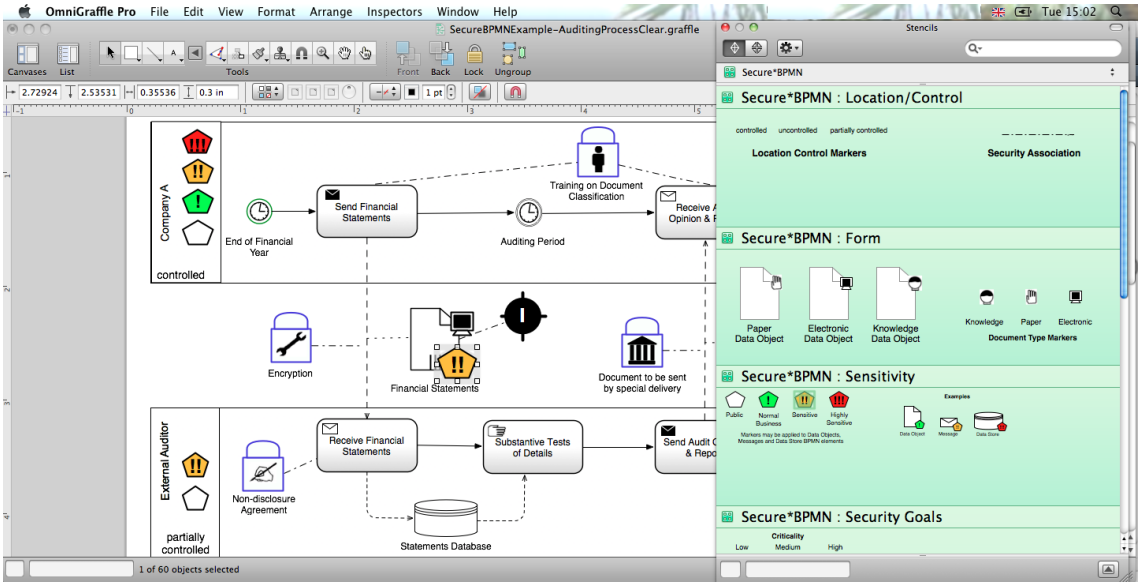


Figure 6.18: Annotation of the financial auditing process using the Secure*BPMN stencil for OmniGraffle.

Figure 6.17 depicts the Secure*BPMN stencil for OmniGraffle. The stencil may be used by dragging and dropping the Secure*BPNM symbols onto a BPMN model. Figure 6.18 shows the annotation of the financial auditing process using the Secure*BPMN stencil for OmniGraffle.

Microsoft Visio Professional also provides a functionality for the development of custom stencils. The Secure*BPMN stencil for Microsoft Visio is visible on the left-hand side of Figures 6.20-6.26. The behaviour of the Secure*BPMN symbols was programmed using the Microsoft Visio

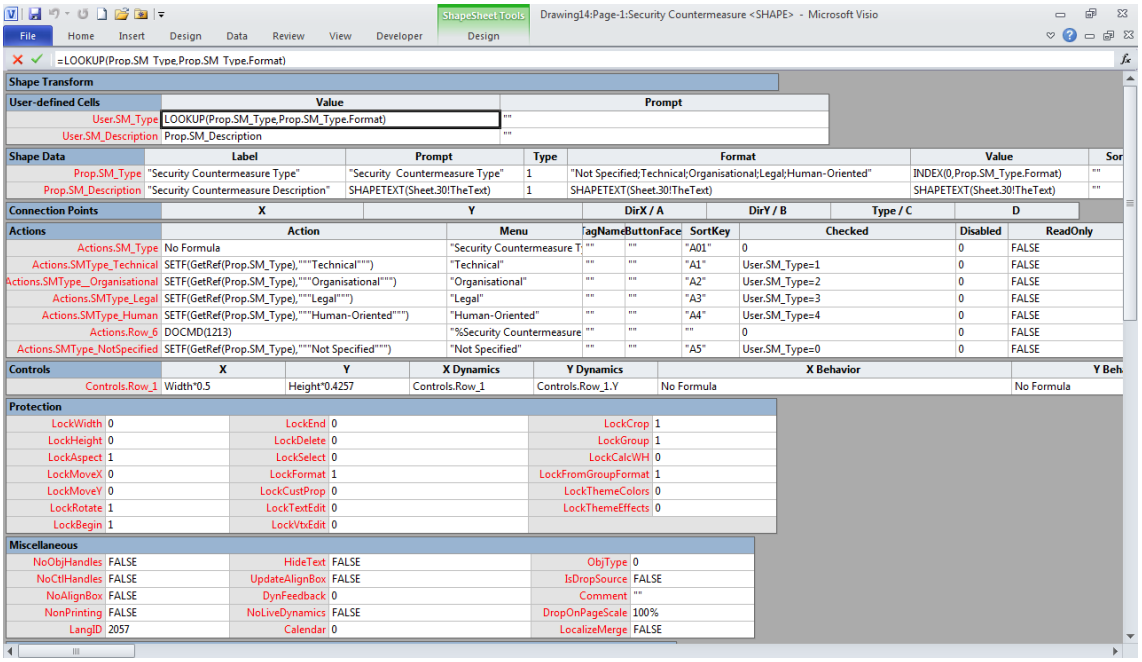


Figure 6.19: Secure*BPMN stencil for MS Visio 2010. ShapeSheet of a security countermeasure symbol.

ShapeSheets[13].

Figure 6.19 depicts the ShapeSheet of a security countermeasure symbol. After dragging and dropping a security countermeasure symbol, a user may use the drop down menu to set up the type of a countermeasure (Figure 6.20). When a countermeasure type is checked in the menu, the appropriate icon appears inside the padlock symbol.

For a security goal, the stencil allows setting up the name and criticality of a goal using the drop down menu as depicted in Figure 6.21. The choice of criticality affects the filling of the shape according to the Secure*BPMN visual vocabulary. The choice of the goal name from the drop down menu results in the appearance of the initial letter(s) of a goal name inside the symbol.

For a Secure Swimlane, the stencil permits the setting up of the location attribute and access permissions as shown in Figure 6.22. The chosen location attribute is depicted below the Swimlane name. Using the drop down menu, a user may specify to which levels of sensitivity a participant has access to. The sensitivity markers which correspond to the sensitivity levels checked at the drop down menu automatically appear on the right of the Swimlane name (Figure 6.22).

[13]In Microsoft Visio each object has a spreadsheet, known as ShapeSheet, which contains information about the object. The ShapeSheet makes it possible to control the behaviour and appearance of the object by inserting formulas and validation rules in the cells of a ShapeSheet.

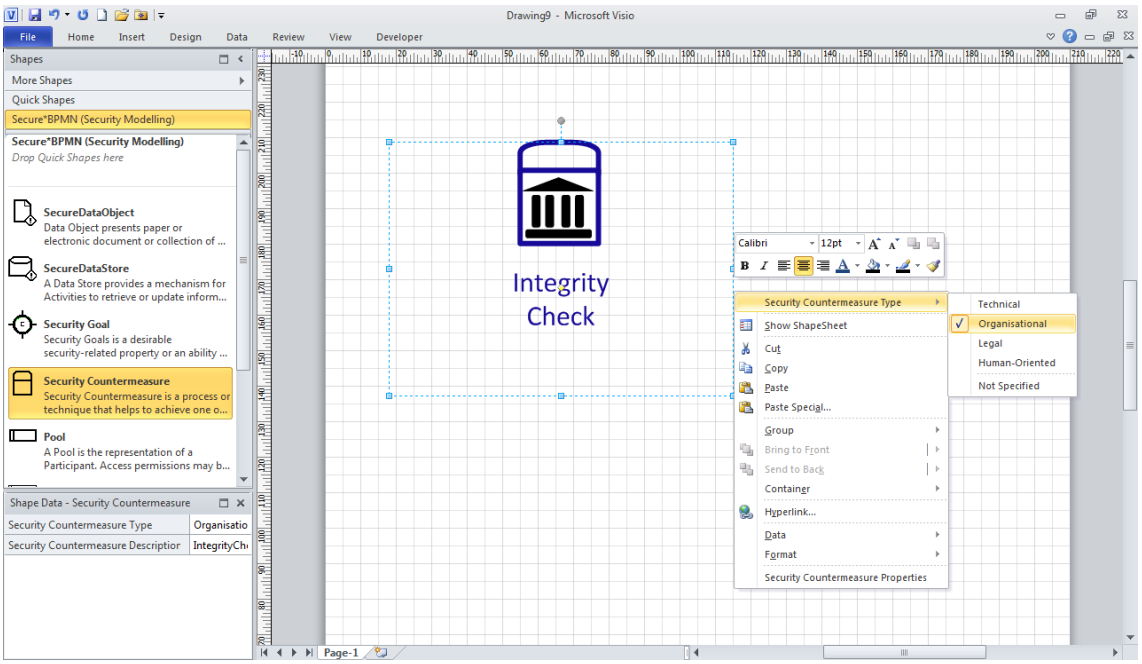


Figure 6.20: Secure*BPMN stencil for MS Visio 2010. Setting up the type of a security countermeasure.

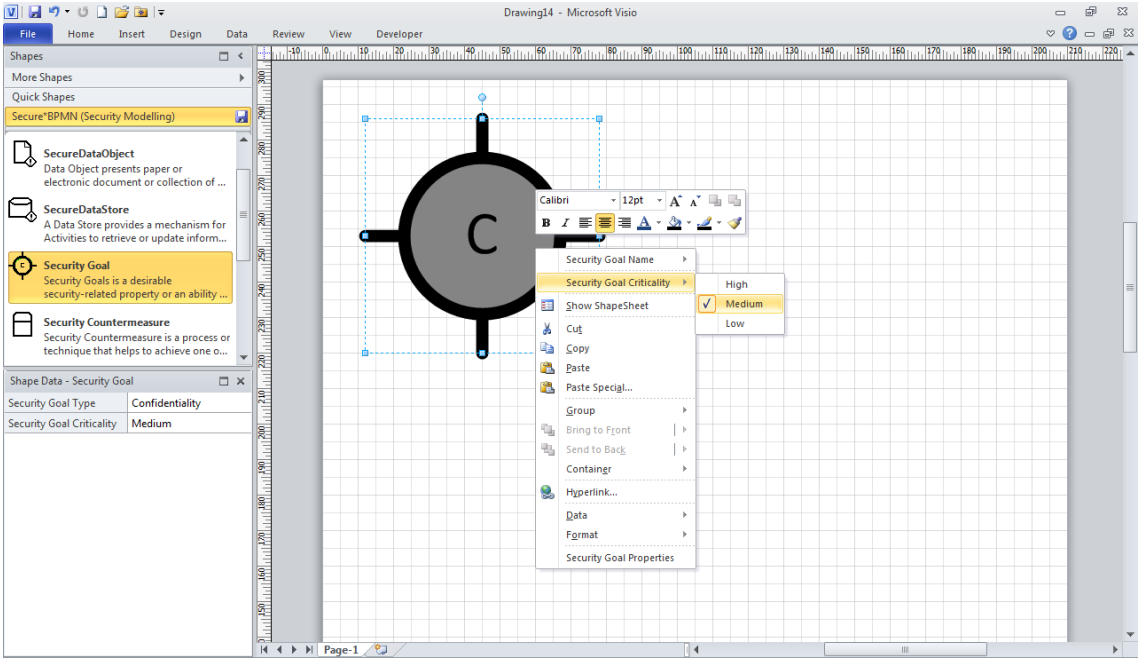


Figure 6.21: Secure*BPMN stencil for MS Visio 2010. Setting up the attributes of a security goal.

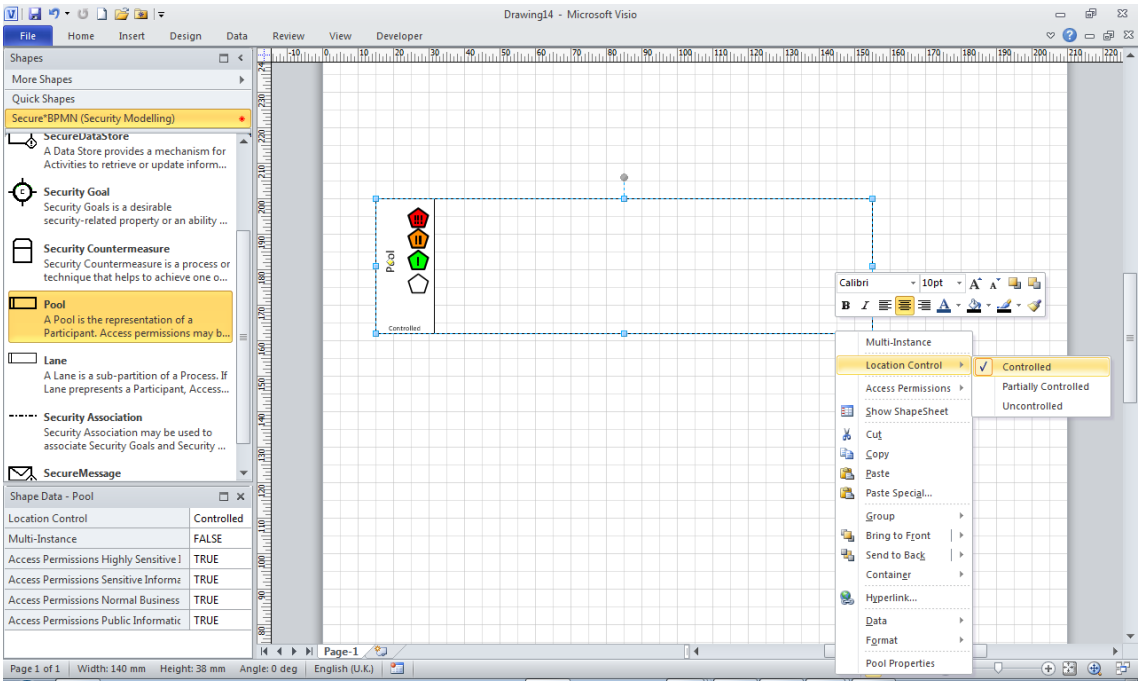


Figure 6.22: Secure*BPMN stencil for MS Visio 2010. Setting up the attributes of a secure swimlane.

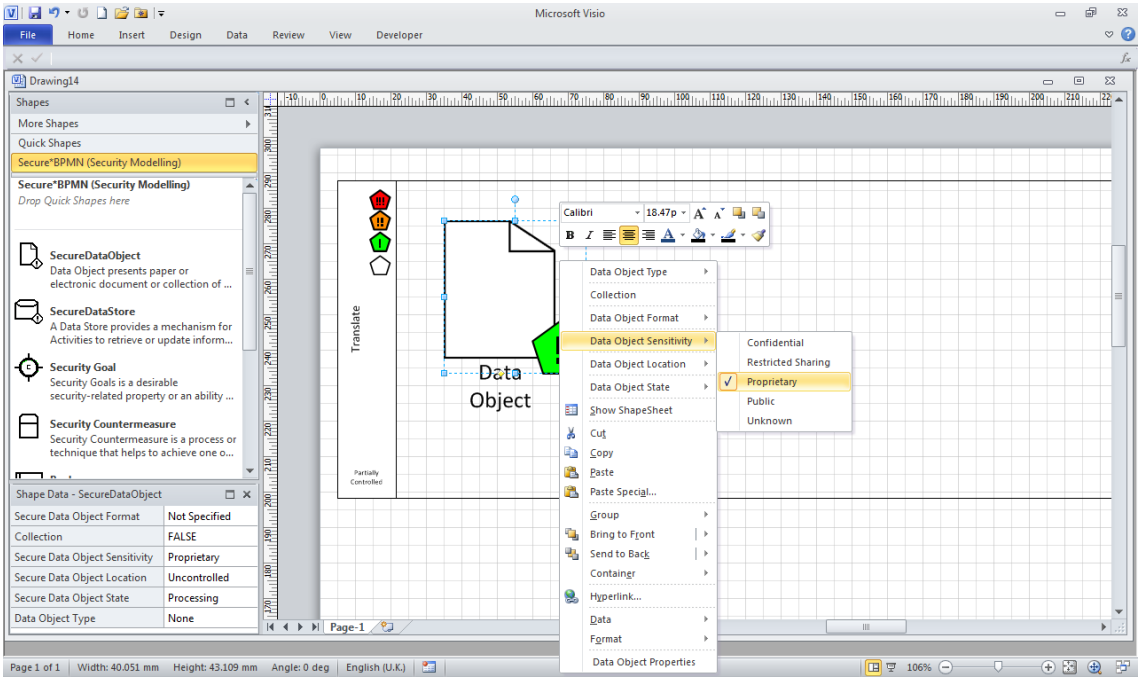


Figure 6.23: Secure*BPMN stencil for MS Visio 2010. Setting up the attributes of a secure Data Object.

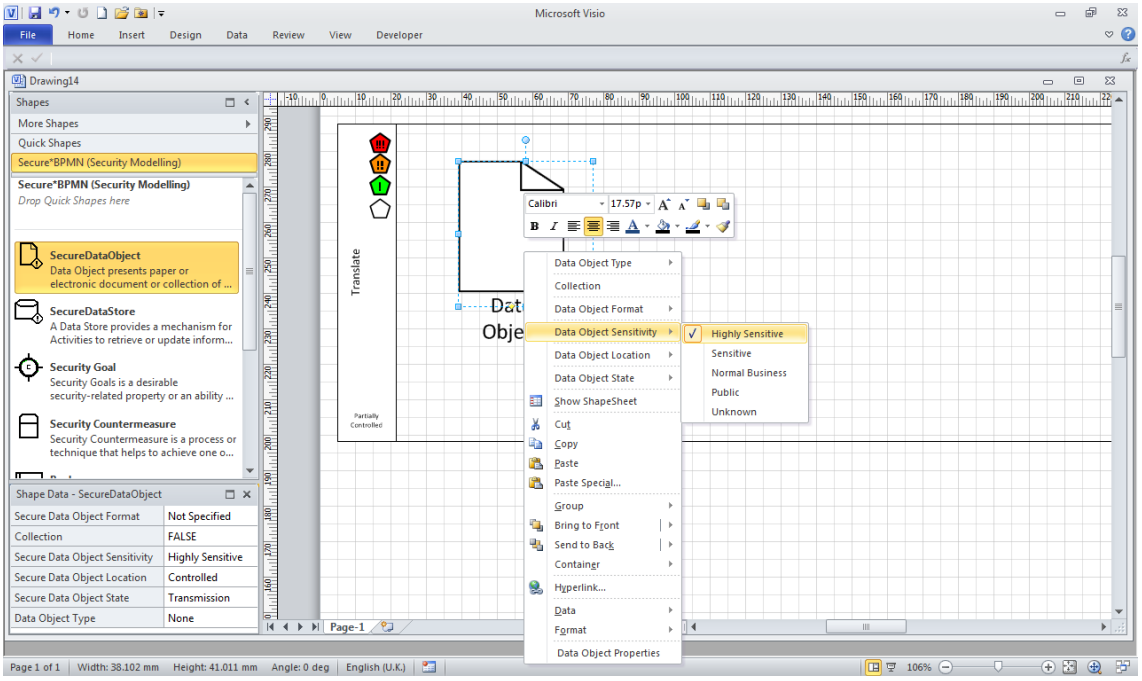


Figure 6.24: Secure*BPMN stencil for MS Visio 2010. Setting up the attributes of a secure Data Object using the Traffic Light Protocol classification scheme.

For a Secure Data Object, the stencil allows the setting of the following attributes: format, location, sensitivity and state (Figure 6.23). In Figure 6.23, a version of Secure*BPMN stencil is shown which is using Translate's document classification scheme (i.e. *Confidential*, *Restricted Sharing*, *Proprietary* and *Public*). However, for another case study a version of Secure*BPMN was created which exploits the Traffic Light Protocol classification scheme (Figure 6.24). This demonstrates the flexibility of Secure*BPMN and the possibility to use the visual grammar with different document classification schemes. On the selection of the required classification level in the drop down menu, the appropriate sensitivity marker appears at the bottom right corner of a Data Object.

For a Data Object the state attribute may be chosen by a user out of five possible options. For a Message element the state is set to *transmission* (Figure 6.25), while for a Data Store for *storage*, according to the Secure*BPMN rules outlined in Table 6.3.

The screen shot depicting the annotation of a procurement business process using the Secure*BPMN stencil for Microsoft Visio 2010 is shown in Figure 6.26.

Since an annotated model may get overburdened with security annotations, both Secure*BPMN stencils support an expert-specific view. An expert may choose a set of security elements to be

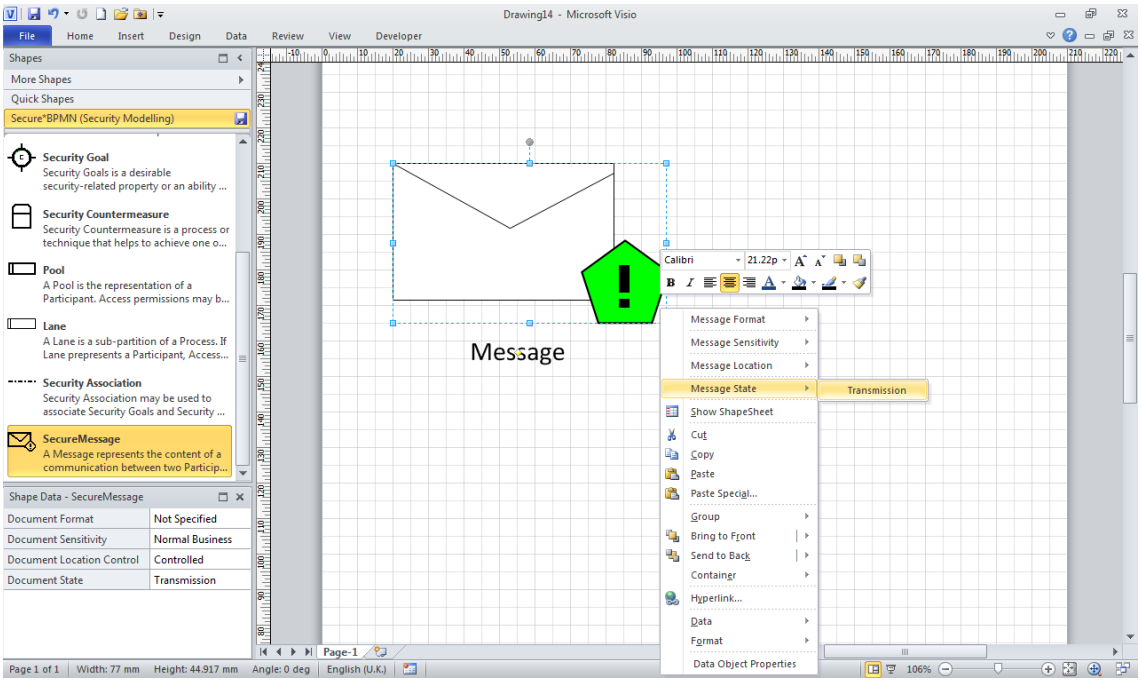


Figure 6.25: Secure*BPMN stencil for MS Visio 2010. The fixed state attribute of a Secure Message.

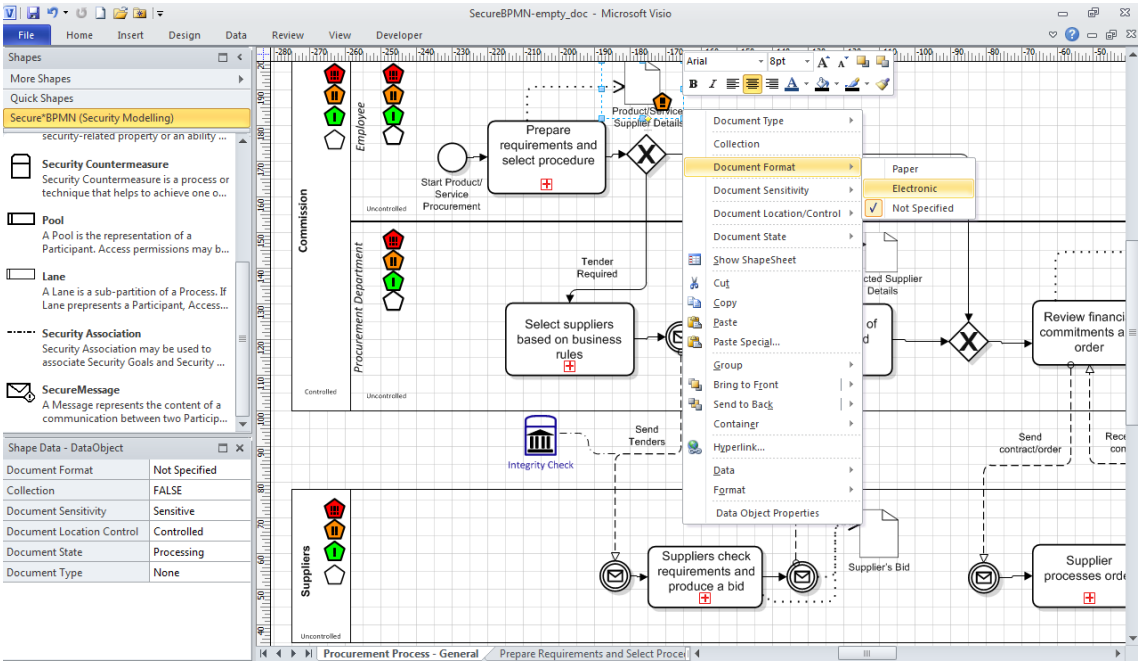


Figure 6.26: Secure*BPMN stencil for Microsoft Visio 2010. The annotation of a procurement business process.

displayed. A business expert may choose to view only the information relevant to him/her (i.e. Data Objects Sensitivity and Security Goals). A legal expert may restrict the mode to depict only legal security countermeasures. This may be done using the inbuilt layering functionality of the diagramming applications.

6.6 Chapter Summary

The main objective of this research project, as declared in Section 1.3, is *to develop a modelling notation that allows the representation of IAS concerns in business process models* (Objective 1.A). In this chapter, where Secure*BPMN is presented, this objective is reached.

Section 1.2, which outlines the problem to be addressed in this thesis, states that there is a need for an easy-to-learn and easy-to-use graphical IAS modelling notation, which is accessible by all members of a multidisciplinary team irrespective of the area of their expertise, and is based upon a shared understanding of the IAS domain among the members of a multidisciplinary team. Secure*BPMN meets the stated desirable characteristics of a sought-for security modelling notation and, hence, addresses the problem formulated.

The novelty of Secure*BPMN lies in its semantics and its syntax. The semantics of Secure*BPMN was based upon the RMIAS which, as proved in Chapter 4, reflects a common understanding of IAS and is suitable for the synchronisation of an approach to IAS in a multidisciplinary team. The syntax of Secure*BPMN was designed specifically for human understanding and communication-enhancement purposes.

In the next chapter, Hypothesis A is tested (Section 1.4). The analytical evaluation is conducted to test the ontological completeness and cognitive effectiveness of Secure*BPMN. Then, the overall effectiveness of Secure*BPMN is tested. It is observed whether experts with different backgrounds and with the different levels of experience in IAS and BPM a posteriori find Secure*BPMN to be a useful and easy-to-use modelling technique, which they are likely to adopt in practice. The differences between Secure*BPMN and other security extensions are also covered in Section 7.5.

Chapter 7

Secure*BPMN Evaluation

The evaluation of the proposed solution is one of the objectives of this thesis (Section 1.3). This chapter is devoted to the evaluation of Secure*BPMN and to testing Hypothesis A (Section 1.4). First, the evaluation methodology is outlined. Next, the ontological completeness (semantics) and the cognitive effectiveness (syntax) of Secure*BPMN are analytically evaluated. Then, the overall effectiveness of Secure*BPMN is empirically tested. After that, Secure*BPMN is compared to the other security-modelling extensions, which are examined in Chapter 5. Finally, the results of the evaluation are discussed and summarised.

7.1 Evaluation Methodology

In this research, specific attention was paid to the evaluation of the proposed security modelling technique, Secure*BPMN. Both types of evaluation - analytical and empirical[1] - were exploited to complement each other.

Figure 7.1 depicts the Secure*BPMN evaluation methodology.

[1]The discussion of these two types of evaluation and their limitations is presented in Appendix A.8.

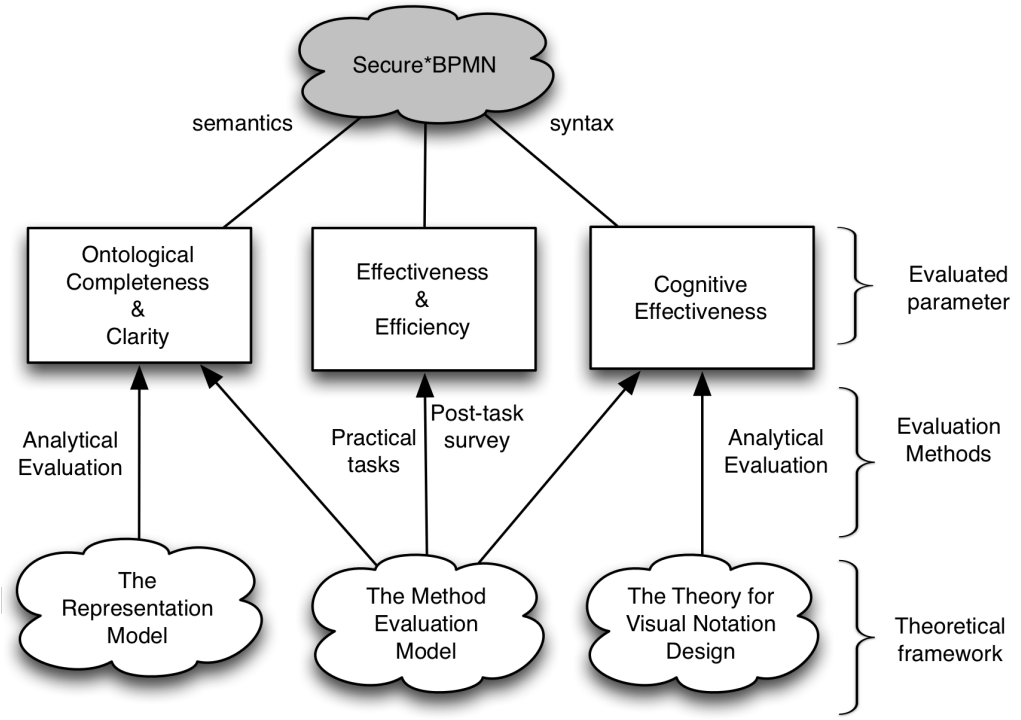


Figure 7.1: The evaluation of Secure*BPMN. Excerpt from Figure 1.2.

The purpose of the evaluation conducted was to test Hypothesis A[2].

The aim of the analytical evaluation was to ensure that Secure*BPMN complies with the formal requirements of the well-established frameworks which are widely used for the evaluation of the quality of modelling languages. The ontological completeness of the semantics of Secure*BPMN was evaluated using the ontological analysis and, specifically, the representation model proposed by Wand and Weber [34, 35, 36]. Section 7.2.1.1 contains the description of the representation model. Section 7.2.1 contains the ontological analysis of Secure*BPMN.

Ontological analysis evaluates the semantics of a notation, but does not address its cognitive effectiveness - "*it focuses on content rather than form*" [30, p.759]. Two notations with identical semantics, but different syntaxes are indistinguishable in terms of ontological analysis. The Theory for Visual Notation Design (TVND) [30] provides a framework for the evaluation of the visual

[2]Hypothesis A: Secure*BPMN is an ontologically complete and cognitively effective modelling notation, which is perceived by experts with different backgrounds and with the different levels of experience in IAS and BPM as a useful and easy-to-use modelling technique which is likely to be adopted in practice (Section 1.4).

aspect and cognitive effectiveness of a modelling language. The TVND is described in Section 7.2.2.1 where the choice of the TVND is also justified. Section 7.2.2 contains the syntactical analysis of Secure*BPMN and presents a discussion on how well the proposed extension meets the requirements of the TVND.

The analytical evaluation of Secure*BPMN, according to the usual practice [13], preceded the empirical evaluation, when Secure*BPMN was applied by a group of prospective users to two practical tasks. The empirical evaluation was design based on the Method Evaluation Model (MEM) [37]. The MEM, along with the justification of its choice, is presented in Section 7.3.1. The purpose of the empirical evaluation was to investigate how easy-to-use and useful the participants of the experiment perceive Secure*BPMN after using it and whether the participants are intended to use Secure*BPMN in future. The empirical evaluation is contained in Section 7.3.

7.2 Analytical Evaluation of Secure*BPMN

7.2.1 Ontological Analysis

7.2.1.1 The representation model

Wand and Weber [34, 191] suggest the representation model which may be used for the evaluation of the ontological expressiveness of a modelling language. In [36], Bunge's ontology of a system is adopted as an exemplary ontology. The representation model used in conjunction with the Bunge ontology is known as the Bunge-Wand-Weber (BWW) model [36, 191].

At present, the representation model is a mature evaluation framework which received a significant amount of scholarly attention in the domain of IS design [30, 165]. The representational analysis is widely employed in process modelling research [159]. The representation model is used for the comparison of modelling languages, quality measurement of models and method engineering [261], but the main area of its application is the ontological analysis of a modelling language in terms of its ability to create a complete and clear picture of a domain being described [162, 262]. In [162], BPMN is analysed using the BWW representation model.

The representation model [191] is concerned with two mappings between a set of real-world concepts captured in an ontological model and a set of semantic constructs in a notation:

- Representation mapping: how an ontological concept is represented via a semantic construct, and
- Interpretation mapping: how a semantic construct stands for an ontological concept.

There are two evaluation criteria in the representation model [191]:

- Ontological Completeness, which reflects the completeness of the coverage of ontological concepts by semantic constructs of a notation and characterises representation mapping, and
- Ontological Clarity, which reflects the degree to which an unambiguous mapping between ontological concepts and semantic constructs of a notation is achieved and characterises interpretation mapping.

The expressive power of a notation depends on the degree of the ontological completeness and ontological clarity a notation has.

The representation model states that a one-to-one correspondence between ontological concepts and semantic constructs should be obeyed. If this requirement is not met then one of four discrepancies may occur:

Construct deficit - no notation construct corresponds to an ontological concept;

Construct overload - a single notation construct represent several ontological concepts;

Construct redundancy - multiple notation constructs represent one ontological concept; and

Construct excess - no ontological concept corresponds to a notation construct.

The construct deficit indicates an ontological incompleteness of a notation, while the other three anomalies indicate the lack of an ontological clarity.

The representation model provides a tool for the comparison of modelling notations by their expressive power. Two notations with equal ontological completeness and clarity are equally expressive. A notation in which less discrepancies occur may be deemed to posses higher expressive power, i.e. to be more ontologically expressive [191, p.234].

7.2.1.2 Ontological Analysis of Secure*BPMN

The representation model is used to evaluate how well Secure*BPMN reflects the IAS domain as it is captured in the RMIAS.

Any notation, independently of an ontology adopted, may be evaluated using the notion of ontological expressiveness [191, p.221]. Although Wand and Weber [36] demonstrate the application of the representation model using a particular ontology, they state that other ontologies may be used in conjunction with the representation model. In this section, the RMIAS plays the role of an ontology.

According to the requirements of the representation model, a bi-directional mapping between the ontological concepts specified in the RMIAS and the semantic constructs of Secure*BPMN was examined.

The full set of ontological concepts was extracted from the RMIAS and is listed in the left column of Table 7.1. The set of Secure*BPMN semantic constructs extracted from the extended metamodel (Figure 6.1 and Table 6.1), is listed in the right column. The corresponding constructs are outlined in the same row.

As Table 7.1 shows, a one-to-one correspondence does not exists between all ontological concepts of the RMIAS and semantic constructs of Secure*BPMN.

Construct deficit[3] occurs for such concept as Driver behind security decisions and, consequently, the Name of the driver, and Security development life cycle and its Stages. Construct deficit indicates the ontological incompleteness of Secure*BPMN. This incompleteness stems from the fact that Secure*BPMN is not a stand alone security modelling technique, but an extension for a business process modelling language. Secure*BPMN only selects and represents the IAS concepts which are relevant from the business processes viewpoint of the IAS domain. Drivers behind security decisions and the security development life cycle with its stages are not included in Secure*BPMN, because they are out of the radar of interest for a multi-disciplinary group looking at the security issues of a specific business process. However, these concepts may be included in security modelling languages which reflect the organisational/managerial or economic perspectives of the IAS domain.

[3] *Construct deficit* - the type of modelling language discrepancy when no notation construct corresponds to an ontological concept.

Table 7.1: Mapping between ontological concepts and semantic constructs

Ontological concept (extracted from the RMIAS (Figure 3.1))	**Secure*BPMN semantic construct** (extracted from the metamodel (Figure 6.1))
Security development life cycle	Not present *
Stages of security development life cycle	Not present *
Information taxonomy	Secure Data
State	State
Form	Form
Location	Location
Sensitivity	Sensitivity
Security goal	Security Goal
Arrow "Prioritise security goals"	(Security Goal) Criticality
The IAS-octave	(Security Goal) Name
Security countermeasure	Security Countermeasure
Security countermeasure type	(Security Countermeasure) Type
Security countermeasure description	(Security Countermeasure) Description
Driver behind security decisions	Not present *
Driver name	Not present *
Not present †	Secure Swimlane
Not present †	Access Permissions
Arrows connecting dimensions	Security Association

* - Construct Deficit

† - Construct Excess

Construct excess[4] is encountered with Secure Swimlane and Access Permission semantics constructs. Construct excess in these two cases is also rooted in the fact that Secure*BPMN is not a stand alone security modelling technique, but an extension for a business process modelling language. That is why additional semantic contracts, which help to link security and business process semantic concepts, are needed. The reasons for the inclusion of additional concepts into

[4]*Construct excess* - the type of modelling language discrepancy when no ontological concept corresponds to a notation construct.

Secure*BPMN metamodel are discussed in Section 6.1.1 and summarised in Table 6.1. Additionally, the criticality of a security goal is not explicitly stated in the RMIAS. However, the right arrow in the RMIAS (Figure 3.1) states "*Prioritise Security Goals*". This assumes that during risk analysis each goal is prioritised and assigned a criticality. As a result, no construct excess occurs in the case of the Criticality construct.

There is no ontological concept in the RMIAS to which more than one Secure*BPMN semantic construct correspond. It means that construct redundancy[5] is not observed in Secure*BPMN.

There is no semantic construct in Secure*BPMN which represents more than one ontological concept. Hence, construct overload[6] does not occur in Secure*BPMN either.

Two discrepancies out of the four outlined in the representation model occur in Secure*BPMN, namely construct excess and construct deficit. It means that both the ontological completeness and clarity of Secure*BPMN are affected. This happens, as explained earlier in this section, due to the fact that Secure*BPMN is an extension to the existing business process modelling language and not an independent security modelling language. Hence, Secure*BPMN must provide a link between business process and security concepts and may only include concepts which are relevant and important in the context of a business process model.

Despite the fact that a concept deficit is observed in Secure*BPMN, in comparison with another modelling extension which also uses the RMIAS as the basis for its semantics [152] (Section 5.4.2.15), Secure*BPMN exhibits a higher level of ontological completeness. While Secure*BPMN represents all ontological concepts of the RMIAS apart form the drivers behind security decisions and security development life cycle, the extension in [152] only represents security goals out of all concepts of the RMIAS (Table 5.6).

Tables 5.5 and 5.6 further show that none of the extensions examined addresses the full set of the ontological constructs of the RMIAS which are addressed by Secure*BPMN. However, there are security concepts which are not addressed by the RMIAS but which are present in other extensions examined, e.g. risk, trust, vulnerability and impact. This stems from a different focus of the extensions and the use of different bases for the semantics. For example, in [181] the extension specifically deals with the issues of trust and depicts trust as a separate concept, in [185] the focus is

[5] *Construct redundancy* - the type of modelling language discrepancy when multiple notation constructs represent one ontological concept.

[6] *Construct overload* - the type of modelling language discrepancy when a single notation construct represent several ontological concepts.

on risk in IS security and therefore, this extension accentuates such concepts as risk, vulnerability and impact. Secure*BPMN did not attempt to cover all concepts found in other extensions, but used the RMIAS as the basis for its semantics which helped to identifying concepts relevant to the audience of a multidisciplinary group of experts targeted by this research.

Wand and Weber [191, p.234] state "*Assuming that the ontological model used in an evaluation for completeness and clarity is 'valid', nothing can be done to improve a grammar's ontological clarity if it is deficient.*" The validity of the RMIAS, used as an ontological model in this analysis, was proved in Chapter 4. The representation model [35] allows making a prediction about a higher expressive power of Secure*BPMN in comparison with other extensions because Secure*BPMN exhibits a greater degree of the ontological completeness than other extensions examined when using the RMIAS as an ontology.

7.2.2 Syntactical Analysis

As explained in Section 6.2.2, the Theory for Visual Notation Design (TVND) [30] provided the guidance for the development of the syntax for Secure*BPMN. This section first contains the description of the TVND and then the detailed syntactical analysis of Secure*BPMN in terms of the nine principles of the TVND.

The design of a cognitively effective syntax involves trade-offs when "*the design can be improved in one respect, but only at the expense of making it worse in some other respect*" [192, p.326]. The trade-offs which were made in Secure*BPMN are also discussed in this section.

7.2.2.1 Theory for Visual Notation Design

The Theory for Visual Notation Design (TVND) [30] is a framework that outlines the properties of a cognitively effective modelling notation. The TVND is also known as the "Physics" of notations. The TVND is based on empirical evidence coming from disciplines such as cartography, graphic design, physiology, linguistics, communication and others.

The choice of the TVND as the theoretical basis for the design of the syntax of Secure*BPMN (Chapter 6) is justified by the numerous advantages of the TVND. Each principle in the TVND consistently declares a desirable property of a cognitively effective notation. The TVND is empirically pre-evaluated as it is created based on empirical evidence. The TVND supports a symbol-by-symbol analysis. The predictions which are developed based on the TVND may be empirically tested. The pragmatic value of the TVND is justified

as the theory already found its way to a wide research community and was applied to a range of notations including Archimate, UML, i*, ORES and others [30, 31]. The cognitive effectiveness of BPMN 2.0 was also analysed using the TVND [31].

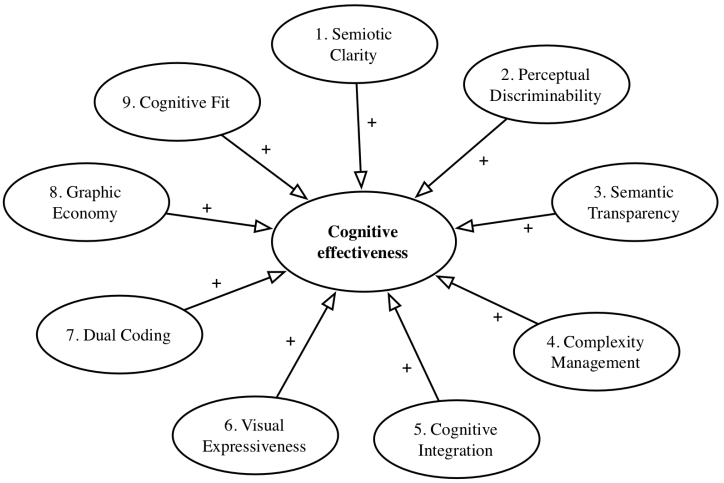


Figure 7.2: The principles of the TVND as variables influencing cognitive effectiveness [30].

The TVND outlines nine principles for optimising the cognitive effectiveness of a notation (Figure 7.2):

1. Semiotic Clarity: There should be a 1:1 correspondence between semantic constructs and graphical symbols;

2. Perceptual Discriminability: Different symbols should be clearly distinguishable from each other;

3. Semantic Transparency: Use visual representations whose appearance suggests their meaning;

4. Complexity Management: Include explicit mechanisms for dealing with complexity;

5. Cognitive Integration: Include explicit mechanisms to support integration of information from different diagrams;

6. Visual Expressiveness: Use the full range and capacities of visual variables;

7. Dual Coding: Use text to complement graphics;

8. Graphic Economy: The number of different graphical symbols should be cognitively manageable;

9. Cognitive Fit: Use different visual dialects for different tasks and audiences.

As an alternative to the TVND, the Cognitive Dimensions of Notations (CDs) framework [192] was considered. The CDs framework declares the principles for the development of visually effective information artifacts. Fourteen dimensions are discussed in [192] and the authors state that new dimensions still emerge.

It means that the earlier versions of the CDs are incomplete, but the newly proposed dimensions are not yet widely accepted and tested by researchers so it is premature to use them as guidances in practice. Another argument against the use of the CDs framework in this research is that it is designed for a plethora of purposes, including the design of word processors, music notation, watches, radios and central heating system controllers. The design of a graphical modelling language is only one of many information artifacts to which the CDs framework may be applied. Due to this generic approach, although some dimensions of the CDs framework are applicable to a graphical modelling notation, others are not relevant (e.g. viscosity, hidden dependences or role-expressiveness). Since it is up to a notation developer to choose which of the dimensions are relevant and should be addressed, this may lead to subjectivity. A dimension which is not well-addressed by a proposed notation may simply be excluded from consideration as an irrelevant aspect. The generic approach adopted in the CDs framework also underlines the vague definition of the dimensions and places extra effort of interpreting the dimensions for a specific artifact on a framework user [31].

While the TVND consistently lists only the principles that should be obeyed by a modelling language, the CDs framework presents a mixture of principles that should be obeyed by a notational system (e.g. the visibility dimension, consistency dimension) and the recommendations on how the notation development process should be undertaken (e.g. the progressive evaluation dimension). The limitations of the CDs framework discussed above (along with other limitations outlined in [31, 30]) guided the author not to chose the CDs framework as the manual for the development of the syntax of Secure*BPMN.

7.2.2.2 Syntactical Analysis of Secure*BPMN

7.2.2.2.1 Principle of Semiotic Clarity. The principle of semiotic clarity states that there should be a one-to-one correspondence between semantic constructs and graphical symbols of a notation.

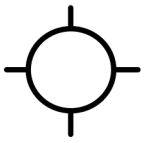
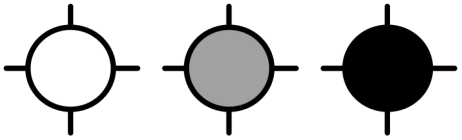
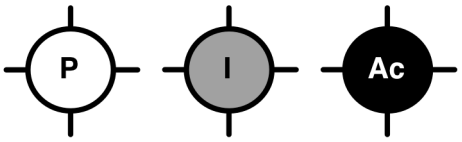
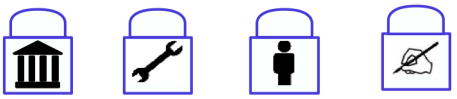
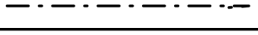
The TVND adopts the one-to-one correspondence principle of the theory of symbols [193]. This principle echoes a one-to-one correspondence requirement of the representation model. However, while the representation model requires a one-to-one correspondence between ontological concepts and semantic (metamodel) constructs, the principle of semiotic clarity requires a one-to-one correspondence between semantic constructs and graphical symbols of a notation.

Table 7.2 shows the mapping between the semantic construct and graphical symbols of Secure*BPMN.

Table 7.2 shows that in Secure*BPMN there is a one-to-one correspondence between the semantic constructs and graphical symbols for the following constructs: Secure Data, Form, Sensitivity, Security Goal, its Name and Criticality, Security Countermeasure and its Type, Access Permissions and Security Association.

Two semantic constructs Location and Security Countermeasure Description do not have graphical representation, but are presented as textual labels/markers. A location is denoted using a text label rather than a

Table 7.2: Mapping between semantic constructs and graphical symbols

Secure*BPMN semantic construct in the metamodel	Secure*BPMN graphical symbol
Secure Data	Data Object (adopted from BPMN)
State	By position in the model
Form	
Location	Textual label (controlled, partially controlled, uncontrolled)
Sensitivity	
Security Goal	
(Security Goal) Criticality	
(Security Goal) Name	
Security Countermeasures	
(Security Countermeasures) Type	
(Security Countermeasures) Description	Textual label under the padlock
Secure Swimlane	Pool or Lane (adopted from BPMN)
Access Permissions	
Security association	

symbol for the reasons discussed in Section 7.2.2.2.8.

Secure*BPMN does not introduce a new symbol to represent the State of information because the syntax of BPMN and the details of a business process model are sufficient to indicate it. The State of a Data Object may be defined based on the position of a Data Object in a business process diagram (Section 6.2.3.7). An introduction of a new graphical symbol in this case would cause symbol redundancy[7], because the information about the State of Data or Message BPMN elements may be extracted from a business process model without an explicit indication of it. In the trade-off between providing extra semiotic clarity in Secure*BPMN by introducing the State marker and reducing graphic complexity by not doing so, it was preferred to avoid bringing additional graphic complexity into Secure*BPMN.

Formally, symbol deficit[8] occurs in Secure*BPMN. However, while according to the ontological analysis and the representation model semantic construct deficit is harmful and indicates the ontological incompleteness, in the context of the graphical notation design symbol deficit is often desirable because it reduces graphic and diagrammatic complexity[9].

In Secure*BPMN the same set of symbols depicts the sensitivity of Data Object and the Access Permissions of a participant. On the one hand, this indicates symbol overload[10] as the same graphical symbol visualises several different semantic constructs. On the other hand, these symbols illustrate close concepts. A sensitivity marker, when used as an access permission marker, indicates the right of access to the information of the shown sensitivity. In this case, in the trade-off between introducing symbol overload or additional graphic complexity the preference was given to the former one in order to reduce graphic complexity.

Symbol redundancy does not occur in Secure*BPMN because there are no instances in Secure*BPMN where more than one symbol represent the same semantic construct.

Symbol excess[11] does not occur in Secure*BPMN either because there is no graphical symbol in the notation that does not have a corresponding semantic construct.

In terms of semiotic clarity, Secure*BPMN demonstrates two anomalies - symbol deficit and symbol overload. However, both of this deficiencies were introduces for the sake of reducing the graphical complexity of Secure*BPMN, which is examined in greater depth in Section 7.2.2.2.8.

[7] *Symbol redundancy* - the deficiency of a modelling notation when several graphical symbols in a notation represent the same semantic construct [30].

[8] *Symbol deficit* - the deficiency of a modelling notation when a semantic construct has no supporting graphical symbol [30].

[9] *Graphic complexity* refers to the number of symbol types in a notation, while *diagrammatic complexity* refers to the number of elements (symbol instances) on a diagram [30, p.765].

[10] *Symbol overload* - the deficiency of a modelling notation when a graphical symbol represent different semantic constructs [30].

[11] *Symbol excess* - the deficiency of a modelling notation when a graphical symbol has no underlying semantic construct [30].

7.2.2.2.2 Principle of Perceptual Discriminability. The principle of perceptual discriminability states that different symbols should be clearly distinguishable from each other.

A diagram is more accurately interpreted if a reader may clearly differentiate graphical symbols. The ease and accuracy with which different symbols are distinguished define the perceptual discriminability of a notation. Discriminability is measured by the visual distance between symbols. The visual distance is characterised by a number of visual variables by which symbols differ and the size of the difference. There are 8 visual variables (elementary graphical techniques) - 2 planar and 6 retinal - that may be used to visalise information [30]. Planar variables are *horizontal position* and *vertical position*. Retinal variables are *shape*, *size*, *colour*, *brightness/darkness*, *orientation* and *texture*. The Secure*BPMN syntax attempts, first, to make its symbols to be easily distinguishable from each other and, second, to achieve the minimal overlap with the BPMN basic elements while maintaining the look-and-feel of BPMN.

Shape plays a key role in discriminability since it is a primary variable for distinguishing visual constructs [30]. It is recommended to adopt shapes from different shape families (e.g. ellipses, quadrilateral) for different semantic constructs [31]. To allow the maximum discriminability between the main Secure*BPMN graphical symbols - security goal and security countermeasure - they are represented by symbols based on shapes from two different shape families: the security goal symbol is a circle-based shape, while the security countermeasure symbol is a rectangle-based shape. Information sensitivity (access permission) markers have a pentagon shape. A pentagon is not among the BPMN basic elements, though it does appear as a marker inside an Event symbol to indicate multiplicity, but as such it only may appear inside a circle shape representing an Event.

Colour is a highly effective visual variable [30]. In Secure*BPMN, redundant colour coding increases the visual distance between a security goal and security countermeasure symbols and enhances their discriminability (a security countermeasure symbol is blue, while a security goal symbol is black). Similarly, sensitivity markers have different colours to enhance their determinability. In both cases, colour is used in a redundant way and may be omitted without a loss of information. The blue colour of a security countermeasure symbol does not code any information and is purely intended for discriminability enhancement. In a sensitivity marker, the colour of the marker supports information coded by the number of exclamation marks inside the marker. (Section 7.2.2.2.6 explains the reasons for the redundant use of colour.)

If an element has at least one unique visual variable it is more easily detected [30]. In Secure*BPMN, the "perceptual pop-out" effect attracts attention to a security goal with high criticality. A symbol of a highly critical security goal is black-filled while none other BPMN or Secure*BPMN symbol has this level of darkness. This makes a highly critical security goal to stand out on a diagram.

Another visual variable - size - is used to enable the discriminability between the BPMN element Event and a security goal symbol. Both elements belong to the ellipses shape family. To avoid confusion the diameter of a security goal symbol must be twice as large as the diameter of an Event. The BPMN specification

does not provide any recommendations on the size of its elements. Therefore, the size of Secure*BPMN elements may be defined only in relation to BPMN elements in a specific diagram.

A security association is depicted by a dash-dot line. This type of line is not in use in BPMN. Therefore, the utilisation of a new type of line helps to enhance perceptual discriminability of security associations.

7.2.2.2.3 Principle of Semantic Transparency.

The principle of semantic transparency recommends the use of symbols whose appearance suggest meaning.

In order to develop an easy-to-use and easy-to-learn syntax, a strong emphasis was made on the semantic transparency of the Secure*BPMN symbols and icons. Semantically transparent symbols and icons are perceived either directly or with minimal training [30]; they elevate intelligibility, especially by a novice audience. The meaning of the Secure*BPMN symbols and icons is expected to become clear and be easily remembered after the rationale behind their design is explained.

The resemblance of a security goal symbol with a target symbol (Figure 6.3) refers to a metaphorical analogy. One of the definitions of the word *target* in the on-line Oxford Dictionary is "*an objective or result towards which efforts are directed*". A security goal is also a desirable property (objective) that is to be achieved in an IS by applying some effort. The effect of semantic transparency in this instance is achieved via the resemblance of concepts.

The padlock shape of a security countermeasure symbol has a connotation to functional similarity between a padlock and a security countermeasure (Figure 6.4a). A padlock is a measure that aims to provide security and, similarly, is a security countermeasure.

The use of icons increases the speed of recognition. Icons are less daunting for human recognition than abstract symbols [30]. In Secure*BPMN icons are utilised as information form markers and security countermeasure type markers. Information form markers (Figure 6.7a), use metaphor associations: a *hand* icon for manually handled paper documents, a *computer* icon for electronic documents processed by machines and a *human head* icon for verbally transmitted information.

The marker for paper documents was elaborated from a BPMN icon used to indicate a manual task. In BPMN, the hand icon is placed horizontally and positioned at the top left corner of a task shape. To satisfy the principle of Graphic Economy (Section 7.2.2.2.8), it was more effective to use an existing BPMN symbol rotated by 90 degrees to depict a closely related concept, than to introduce a new icon.

The markers indicating the type of a security countermeasure refer to the following metaphors and functional associations: (1) an official building is a place where an organisation is usually based, (2) a human figure refers to actions involving a person as an individual, (3) a spanner gives an association with technical solutions, and (4) a hand holding a pen refers to signing a contract and concluding a legal agreement.

It is considered hard to visualise the associations between BPMN elements in a semantically transparent way [31]. In Secure*BPMN, the security association line does not have any semantic load, but differs from other types of line in BPMN to avoid confusion and enable perceptual discriminability.

In information sensitivity markers cultural associations are used. An exclamation mark in written text highlights the importance of a sentence and multiple exclamation marks aim to attract an increased attention to a particular piece of information. An exclamation mark appears in road signs which warn about a danger. The red colour is also associated with danger [30] in Western cultures (North America and Europe). In Secure*BPMN, a symbol of red colour and with three exclamation marks inside denotes the highest level of sensitivity in a document classification scheme.

The meaning of colour is culture-specific. Therefore, it is recommended to revise the colours of sensitivity markers in the versions of Secure*BPMN which are to be used in countries where colours have connotations different from those in Western cultures. It is out of the scope of this thesis to design country- and culture-specific versions of Secure*BPMN.

7.2.2.2.4 Principle of Complexity Management.

The principle of complexity management requires a notation to depict information without overloading the reader's mind. Complexity management is an obstinate issue in the field of visual notations design [30].

Secure*BPMN, as with any extension attempting to enrich BPMN with additional information, increases both the graphic complexity and diagrammatic complexity[12] of the modelling language. Complexity significantly affects the intelligibility and readability of annotated diagrams. Since it is essential to make security-annotated diagrams clear and easy to interpret, it is necessary to manage the complexity of Secure*BPMN-annotated models effectively.

As a confirmation of the importance of addressing the complexity of security-annotated diagrams, the problem of increasing diagrammatic complexity sparked an intensive discussion at the 4th International BPMN 2012 workshop, where the first draft of the Secure*BPMN syntax was presented [26]. The audience was questioned about the clarity of a security-annotated model and the session chair Jan Mendling invited the audience to vote. The audience was split approximately as follows: 40% admitted the annotated model to be complex and hard to understand, while 60% agreed that the model is accessible and easy to grasp. (Due to the fact that the voting was unplanned the precise numbers were not calculated; the given numbers are approximate and based on observation.) The audience at the BPMN 2012 conference included BPMN professionals and researchers (people who are well familiar with BPMN), but the complexity of annotated diagrams was still a concern for a significant part of the audience.

[12] Diagrammatic complexity is measured by the number of symbols in a diagram. Graphic complexity is measured by the number of symbols in a notation [30].

This section shows how the diagrammatic complexity of security-annotated BPMN models may be managed (graphic complexity is discussed in Section 7.2.2.2.8). First, the inbuilt complexity management mechanisms of BPMN are discussed and then the characteristics of BPMN models suitable for security annotation.

The mechanisms for managing complexity in BPMN 2.0. BPMN 2.0 includes several mechanisms for coping with complexity, namely decomposition (sub-processes) [9], the use of different types of diagrams and the different levels of abstraction [31]. These mechanisms may be effectively used in security-annotated diagrams. For example, a model may be reduced in size by adopting a more abstract viewpoint.

An activity, where security issues are multiple and complex, may be presented as a sub-process. The sub-process shows a more detailed version of the process accompanied by security annotations. A sub-process supports vertical decomposition.

Horizontal decomposition, which deals with complexity at the same level of abstraction, is supported in BPMN 2.0 by a Link Event that serves as a connector between different diagrams presenting parts of the same process or related processes.

Four types of diagrams in BPMN allow the representation of information only relevant to a specific viewpoint, ignoring irrelevant details or adding required details. For example, a multiple exchange of messages may be presented as a conversation diagram for a purpose where the details of a message exchange are unimportant [160, p.124]. From the legal perspective, it is important that an exchange of sensitive information will take place and, therefore, a non-disclosure agreement must be in place, but the details of the actual message exchange are irrelevant.

Therefore, Secure*BPMN does not include any specifically-developed mechanisms for managing complexity, but relies on the mechanisms inbuilt in BPMN because they are sufficient.

BPMN diagrams suitable for security annotation. The understandability of a business process model destined for security-annotation dramatically affects the understandability of a final security-annotated diagram. It is important to choose for security-annotation only BPMN diagrams that are readable and comprehensible.

One of the features of a business process model (and, in fact, of any model of reality) is to abstract from details which are not essential for a modelling purpose [9]. Within the limited and precious space of a diagram, only aspects of a business process which are relevant to a specific modelling goal and to a specific group of readers must be presented. In security-annotated diagrams, the secondary details of a business process which are not relevant to IAS may be omitted for increasing the intelligibility of a model.

In order to achieve the intelligibility of business models annotated with security details, typical quality problems found in business process models which hinder their understandability must be avoided. The

typical quality problems include inconsistent labelling, redundant process fragments and unnecessary large size and complexity of models [156, 194].

The size[13] is the most important metric of a business process model affecting its understandability [194]. The critical role of the size of a model is explained by the fact that the limited cognitive capabilities of humans do not allow the effective tracking of interrelationships in large-size models and may lead to errors [194]. Therefore, it is recommended to use for security-annotations business process models that are small in size. Small-size business process models are less prone to errors and more effective for communication purposes [194]. No recommendations was found in the literature with regard to the comprehensible size of BPMN models. However, drawing on more general observations outlined in [196], it is recommended that the number of activities in BPMN models which are destined for security-annotation must be 7 ± 2.

Although the rich syntax of BPMN allows the development of complex business process models, the users' feedback indicates that in practice simpler, smaller size models prevail and are preferred to more complex ones [159]. This thesis suggests that a complex BPMN diagram destined for security-annotation must be consistently decomposed into smaller models, while not loosing important details in a fragmented process and only then annotated with security detail to help the readers of an annotated model.

Size is only one of the metrics of the business process model complexity and intelligibility [195]. For a model which is destined for Secure*BPMN-annotation, it is also recommended to reduce the complexity of the following metrics: the number of possible control flow decisions [195], maximum/mean nesting depth [195] and density [194].

7.2.2.2.5 Principle of Cognitive Integration.

The principle of cognitive integration requires a notation to include mechanisms to support the integration of information from different diagrams.

As with complexity management, for cognitive integration Secure*BPMN relies on the mechanisms inbuilt in BPMN (e.g. a BPMN Link Event which enables a linkage between different diagrams [31]). Although, it is established that BPMN does not provide effective ways of dealing with cognitive integration [31] (e.g. summary diagram, contextualisation, identification, navigation map [30]), it is out of the scope of Secure*BPMN to introduce new ways of coping with cognitive integration into BPMN.

7.2.2.2.6 Principle of Visual Expressiveness.

The principle of visual expressiveness prescribes the use of the full range and capacities of visual variables for maximising cognitive effectiveness.

Visual expressiveness characterises visual variations across the visual vocabulary of a notation and is measured on a scale from 0 to 8 as the number of visual variables used in a notation. While 0 indicates a non-visual (textual) notation, 8 indicates a visually saturated notation where all existing variables are in

[13] The size of a business process model is characterised by the number of activities in a model [195].

use. The set of all visual variables is split into two groups: (1) information-carrying variables and (2) free variables (those that do not encode any information).

On the scale of visual expressiveness Secure*BPMN scores 6 because it uses 6 out of 8 visual variables (Figure 7.3):

- *Shape* to encode the nature of a security element (circle, rectangle, pentagon);
- *Brightness* to indicate the criticality of a security goal;
- *Colour* to indicate the sensitivity of information (white, red, amber, green) and for the enhancement of the security countermeasure symbol discriminability (blue);
- *Size* of a security goal symbol to improve distinguishability from an Event BPMN element;
- *Horisontal position* and *vertical position* to place a Secure*BPMN marker over a BPMN element (e.g. top right corner of a Data Object to position an information form marker), to enclose an icon in a security countermeasure symbol and exclamation mark(s) into a sensitivity marker.

Free visual variables in Secure*BPMN are orientation and texture.

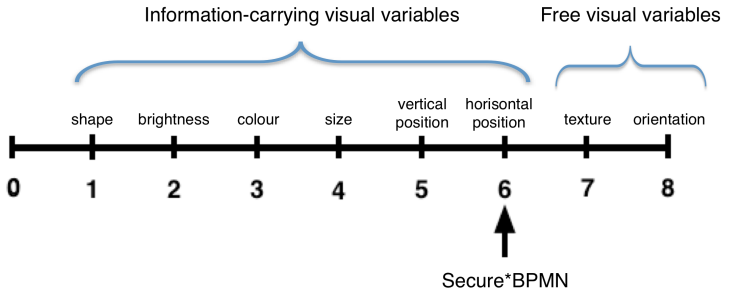


Figure 7.3: Visual Expressiveness of Secure*BPMN

The syntax of BPMN contains 171 symbols, but uses only four out of eight visual variables (Visual Expressiveness of BPMN = 4) [31]. Secure*BPMN demonstrates a higher level of visual expressiveness even with a lower number of symbols in a notation, which makes it more visually expressive.

Table 7.3 analyses the coverage of the design space by Secure*BPMN. Capacity is a number of perceptible steps for a specific visual variable. The capacity values are adopted by the TVND from psychophysics research. Saturation shows the percentage of the variable's capacity occupied by the Secure*BPMN syntax. Table 7.3 shows that Secure*BPMN uses a significant fraction of the design space for such visual variables as darkness and colour, but still leaves a room for further extensions. Colour has the potential to be used in more extensive information classification schemes with up to ten levels of information sensitivity. Brightness has only 42-50% saturation, which means that the Secure*BPMN syntax may be extended to categorise the criticality of a security goal finer-grained than "*low, medium and high*" and to include up to seven levels

of criticality. Size has low saturation. Since the capacity of size is underused, the use of size in practice may be increased to enhance the discriminability of Secure*BPMN elements or/and improve understandability of annotated diagrams.

Table 7.3: The coverage of the design space by Secure*BPMN

Variable	**Capacity** [30]	**Secure*BPMN variables**	**Saturation**
Shape	Unlimited	Rectangle-based, circle-based, pentagon	-
Darkness	6-7	Low, medium, high	42-50%
Colour	7-10	White, red, amber, green, blue	40-57%
Size	20	Size of a security goal symbol in comparison with an event element	5%
Horizontal position	10-15	Enclosure of icons, Position of markers	13-20%
Vertical position	10-15	Enclosure of icons, Position of markers	13-20%

To enhance visual effectiveness, the shapes of security goal and countermeasure symbols in Secure*BPMN are iconic. The use of iconic shapes, according to the TVND, is preferred. As recommended by the TVND, colour in Secure*BPMN is used in a redundant way (robust design) [30]. It makes Secure*BPMN suitable for colour-blind people and applicable in black-and-white modes (e.g. black-and-white printers). Another reason for the redundant use of colour in Secure*BPMN is the avoidance of clashes with proprietary conventions of software tools supporting modelling in BPMN. Since the BPMN specification [160] does not dictate any rules about colour, colour is often used in BPMN software tools as a cognitive helper in a non-standardised way [31].

7.2.2.2.7 Principle of Dual Coding.

Although it is not recommended by the principles of perceptual descriminability and visual expressiveness to use text to distinguish symbols because it is cognitively ineffective, in practice text is often used in IS modelling techniques [30] (e.g. UML class diagram). The complexity of problems represented forces the use of text. It may be hypothesised than for an individual it is easier to process text despite its cognitive ineffectiveness, that to maintain in memory an extensive graphical vocabulary.

To address this issue, the principle of dual coding recommends the use of text to complement graphics, rather than to substitute them. Text accompanying a symbol expands, clarifies and reinforces the meaning of the symbol [30].

Taking into account a broad range of available security countermeasures, it is not effective to introduce a separate symbol or icon for each of them (there are over 20 security countermeasures enumerated in Appendix A.7 as a non-exhaustive list). Although it is technically possible to produce a unique icon for each security countermeasure, it may only be done at the expense of Graphic Economy (Section 7.2.2.2.8). The effort required to learn numerous iconic markers would not make the use of a discrete symbol for every security countermeasure effective for the purposes of Secure*BPMN.

Following the above consideration, the name of a security countermeasure instance is indicated by a label

underneath a security countermeasure symbol. This combination is effective according to the TVND. The text is used to distinguish between instances of a security countermeasure and a symbol to differentiate the type of a security countermeasure. Similarly, the name (instance) of a security goal is indicated using a textual label (corresponding letter(s) of a goal type name) in the middle of a security goal symbol.

7.2.2.2.8 Principle of Graphic Economy While the principle of complexity management addresses diagrammatic complexity, the principle of graphic economy deals with the graphic complexity of a notation, defined by the number of symbols in a notation.

The range of visual variables enables the creation of a large amount of graphical symbols. Unfortunately, this potential cannot be fully realised because there is a cognitive limit on the number of symbols that may be effectively recognised by a human [30]. Graphic complexity hinders the understanding of diagrams, particularly by novice readers [30]. Therefore, graphic complexity has to be dealt with and it is often done by compromising on semiotic clarity and perceptual descriminability.

Formally, BPMN is graphically a very complex modelling language because it includes 171 different symbols [31]. Nevertheless, in practice, the full vocabulary of BPMN is rarely used [11]. In reality, only a limited set of around ten basic BPMN elements is in use [11]. This is particularly true in the operational BPMN models used for documentation and analysis purposes which serve as a basis for Secure*BPMN annotation. This means that Secure*BPMN icons in reality will be used in a conjunction with 10 BPMN elements, rather than all 171. This assumption significantly reduces the overall expected graphic complexity of BPMN extended with security modelling capabilities.

The graphic complexity of Secure*BPMN is 15. It is calculated as follows:

- security goal - 3 symbols (1 symbol with different darkness);
- security countermeasure - 4 symbols (1 symbol with 4 changing icons);
- information form markers - 3 icons;
- information sensitivity markers - 4 icons; and
- security association line - 1 symbol.

Hence, the overall graphic complexity of security-annotated BPMN diagrams is 25. Since the language becomes complex, Secure*BPMN uses the following ways to reduce graphic complexity (as recommended by the TVND):

- Increases its visual expressiveness (as discussed in Section 7.2.2.2.6), and

- Introduces symbol deficit. The symbol deficit for the state attribute is discussed in Section 7.2.2.2.1. A location of a swimlane is denoted using a text label, rather than a symbol. In this instance Secure*BPMN uses a visually ineffective text annotation and compromises on visual expressiveness and discriminability for the sake of graphic economy.

7.2.2.2.9 Principle of Cognitive Fit. The principle of cognitive fit recommends using different dialects for expert and novice audiences as well as for different representational medium.

Secure*BPMN was designed to be suitable for novice users. In order to make it suitable for a novice audience, methods recommended by the TVND were used, namely well discriminable symbols, mnemonic conventions (use of icons) and explanatory text. For further simplification for novice users, a limited visual vocabulary may be recommended which includes only two graphical symbols - a high criticality security goal symbol and a security countermeasure symbol (with no icon inside). Although this limited visual vocabulary does not allow the expression of all security related concepts and their attributes identified in the RMIAS, the main IAS concepts - a security goal and a security countermeasure - may be expressed.

Secure*BPMN, with its use of darkness and colour, was developed to utilise the graphic capabilities of modern modelling software tools. Nevertheless, while working on the syntax of Secure*BPMN, it was taken into account that a security-annotated BPMN diagram may be delivered on a different representational medium, e.g. whiteboard or paper.

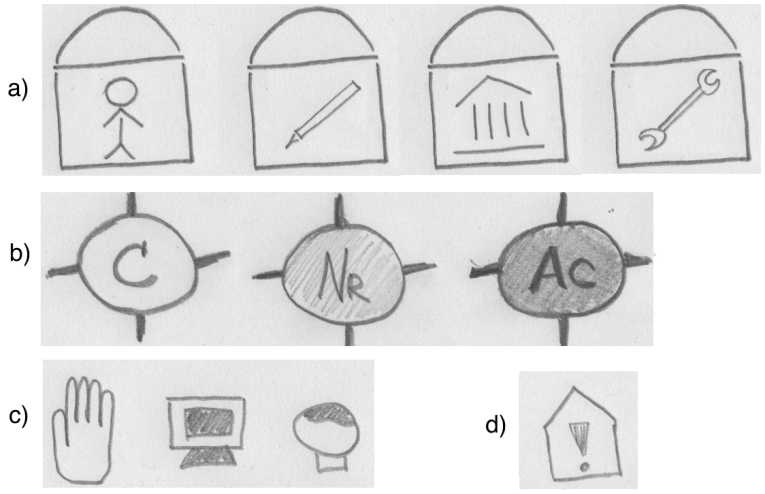


Figure 7.4: The hand-drawn Secure*BPMN symbols

Colour, as discussed in Section 7.2.2.2.6, is used in Secure*BPMN in a redundant way. Therefore, Secure*BPMN is suitable for a monochromatic medium (e.g. a black-and-white printer).

There may be situations when Secure*BPMN-annotation is done by hand (e.g. on paper or a blackboard). The symbols of a security goal and security countermeasure are easy to draw by hand (Figure 7.4a,b). The pentagon of a sensitivity marker is easier to hand-draw in a shape of a house, rather than a regular

pentagon (Figure 7.4d). The most difficult for hand-drawing are icons. The Secure*BPMN icons require simplification to be better suited for hand-drawing. The simplified versions of the Secure*BPMN icons are presented in Figure 7.4a. A *hand holding a pen* icon of a legal security countermeasure is substituted with a *pen* icon. The criticality of a security goal symbol when drawn by hand may be indicated by no hatching, hatching and cross hatching for low, medium and high criticality respectively (Figure 7.4b).

7.3 Empirical Evaluation of Secure*BPMN

7.3.1 The Method Evaluation Model

The Method Evaluation Model (MEM) [37] was chosen as a theoretical framework for the empirical evaluation of Secure*BPMN due to the following considerations. The MEM builds upon and adapts the Technology Acceptance Model (TAM) [197] for the evaluation of a modelling language or method. The TAM is a well accepted in the IS literature as a theoretical model for the evaluation of technology acceptance [37]. Moody, the author of the MEM, argues that there are similarities between technology acceptance and adoption of a method in practice because both of these are reasoned decisions taken by practitioners as a result of some activities [37]. Therefore, it is legitimate to adjust the TAM for the evaluation of the method/modelling language acceptance. In [167], BPMN is evaluated using the adjusted version of the TAM. Recently, the MEM is actively used as a framework for the comparative evaluation of security-modelling languages [201, 202, 263, 264].

The MEM consists of six constructs (Figure 7.5):

1. Actual Efficiency: the effort required to apply a method;
2. Actual Effectiveness: the degree to which a method achieves its objectives (O);
3. Perceived Ease of Use: the degree to which a person believes that using a particular method would be free of effort;
4. Perceived Usefulness: the degree to which a person believes that a particular method will be effective in achieving its intended objectives;
5. Intention to Use: the extent to which a person intends to use a particular method; and

6. Actual Usage: the extent to which a method is used in practice.

Table 7.4: The definitions of the MEM constructs adjusted for Secure*BPMN

Construct	Definition in [197]	Definition in [167]	Definition in this thesis
Perceived Usefulness (PU)	The degree to which a person believes that using a particular system would enhance his or her job performance.	The degree to which a person believes that a particular process modelling grammar will be effective in achieving the intended modelling objective.	The degree to which a person believes that Secure*BPMN will be effective for security-annotation of BPMN models.
Perceived Ease of Use (PEOU)	The degree to which a person believes that using a particular system would be free of effort.	The degree to which a person believes that using a particular process modelling grammar would be free of effort.	The degree to which a person believes that using Secure*BPMN would be free of effort.
Intention to use (ItU)	The extent to which a person intends to use a particular system.	The extent to which a person intends to continue to use a particular process modelling grammar for process modelling tasks.	The extent to which a person intends to continue to use Secure*BPMN for security-annotation of BPMN models.

Perceived Ease of Use, Perceived Usefulness; and Intention to Use are constructs of the TAM. Table 7.4 outlines the definitions of these three constructs as adopted in (a) the TAM [197], (b) in [167], where the TAM is applied for the BPMN acceptance evaluation, and (c) in this work, as adjusted for the context of the Secure*BPMN.

The effort needed to apply a method defines Actual Efficiency of a method and could be measured, for example, in terms of time or cost [37]. Actual Efficiency influences Perceived Ease of Use. Actual Effectiveness reflects how well a method achieves its objectives and may be measured in terms of the quantity or quality of the results. Actual Effectiveness influences Perceived Usefulness. Perceived Ease of Use affects Perceived Usefulness [197], and together they impact Intention to Use, which in its turn determines Actual Usage.

The MEM shows that Actual Efficiency and Actual Effectiveness affect the Intention to use and subsequently Actual Usage only via perceived Ease of Use and Perceives Usefulness. Perceived variables are subjective, which only to a certain degree are defined by the actual performance, and are also influence by other parameters such as personal preferences, knowledge of other methods, background etc.

Figure 7.5 shows the adaptation of the MEM for the evaluation of Secure*BPMN. There are six constructs in the MEM: Actual Efficiency, Actual Effectiveness, Perceived Ease of Use, Perceived Usefulness, Intention to Use and Actual Usage. The definitions of these constructs along with the version of the definitions adapted to the context of Secure*BPMN are presented in the last column of Table 7.4. Time needed to apply Secure*BPMN defines its Actual Efficiency. Actual Efficiency influences Perceived Ease of Use. Actual Effectiveness, which is characterised by the correctness of the results, influences Perceived Usefulness.

Perceived Ease of Use affects Perceived Usefulness. Perceived Ease of Use and Perceived Usefulness together impact Intention to Use, which in turn determines Actual Usage [37, 197].

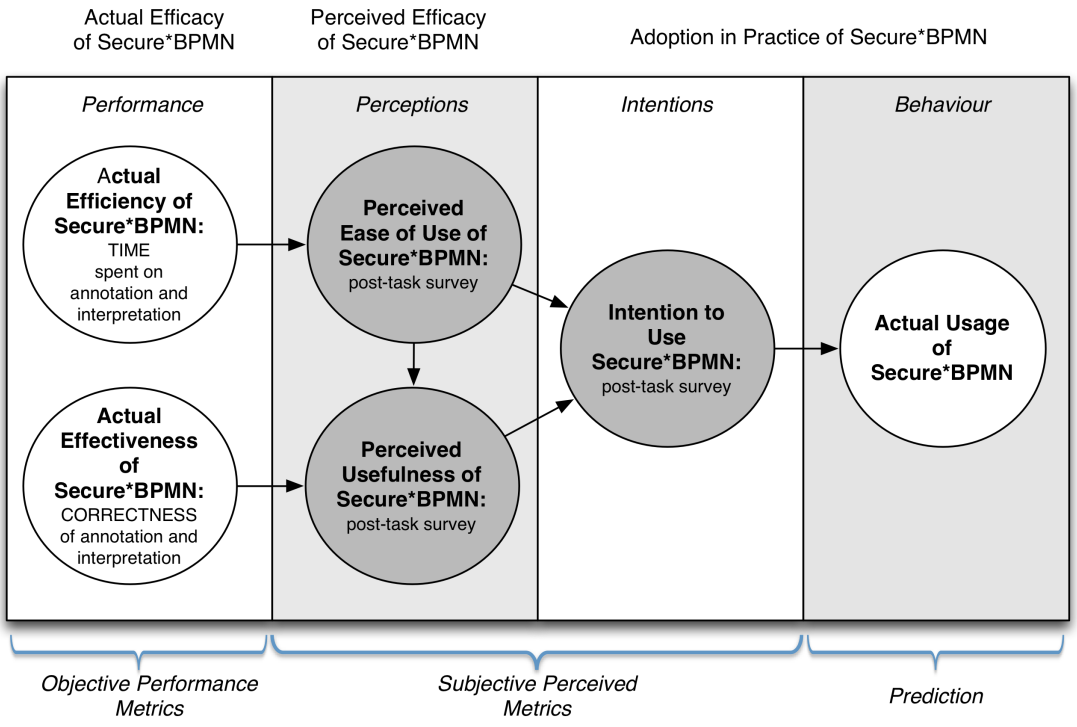


Figure 7.5: The Method Evaluation Model [37] as adapted for the evaluation of Secure*BPMN.

7.3.2 Experimental Design and Procedure

The evaluation experiment consisted of three main parts:

1. Training on Secure*BPMN - the participants were given a one-hour training session on Secure*BPMN;
2. Practical Tasks - since for a successful application of Secure*BPMN a user must be able to annotate a BPMN diagram using the modelling technique and to read an annotated diagram, it was suggested that participants performed two practical tasks:

   (Task 1) - Annotation of a BPMN diagram using Secure*BPMN; and

   (Task 2) - Interpretation of a diagram annotated using Secure*BPMN;
3. Post-task survey - the participants were asked to provide their opinion regarding the use of Secure*BPMN.

The design of the experiment is similar, with some adaptation to the context of Secure*BPMN, to the one in [37], where participants are given a training on a modelling technique, knowingly perform task(s) using the technique and then express their opinion in a post-task survey.

The pilot test of the experiment was performed with two PhD students and two academics who were fully aware about the settings and goals of the experiment. The tasks, diagrams and survey were corrected reflecting the feedback received in the pilot test in order to improve the clarity of the written material.

Two groups of participants were involved in the evaluation experiment: the group of 16 professionals and the group of 15 MSc students. Twenty seven participants took part in the experiments in person. Four participants, due to their schedule or location, were not able to participate in a workshop in person and took part in the experiment remotely. Each participant received by an email the slides used in training sessions, the detailed instructions on how to perform the tasks and all written material required for the experiment. For the annotation task, a participant was expected to print out the material, to annotate a sample BPMN diagram and to send an annotated diagram to the author by email as a scanned image or by post.

Table 7.5 summarises the details of the conducted workshops.

Table 7.5: The details of the conducted Secure*BPMN workshops

Date	**Venue**	**Audience**	**Training Length**	**Number of Responses**
6 14.10.13	Cardiff University	Researchers, PhD students and practitioners	1 hour 30 minutes	5
06.11.13	West of England University	Software Engineering Researchers and Practitioners	45 minutes	2
14.11.13	Cardiff University	IAS professionals	1 hour 20 minutes	3
21.11.13	Cardiff University	Information Security and Privacy MSc students	1 hour	17
-.11.13	remotely	Researchers and practitioners	n/a	4

For consistency, throughout the experiment a case-study of Translate was used. Translate is introduced in Appendix A.5.

Two types of metrics were collected in the experiment as suggested by the MEM:

- *Objective performance-based metrics*:

  1. The **Time** spent by a participant on each task.

     The time which was spent on the completion of each task was measured and reported by a participant in the post-task survey. Time is a measure of Actual Efficiency [37].

  2. The **Correctness** of the tasks performance.

     The correctness of the task performance was measured by the author. The marking scheme for Task 1 is presented in Appendix A.17. The marking scheme for Task 2 is presented in Appendix A.19. The correctness of the tasks performance is a measure of Actual Effectiveness [37].

- *Subjective perception-based metrics*:

  1. **Perceived Ease of Use** (PEOU),
  2. **Perceived Usefulness** (PU) and
  3. **Intention to Use** (ItU).

  These metrics were reported by the participants in the post-task survey.

Intention to Use, which was expressed by the participants in the post-task survey, might help to estimate the likelihood of the adoption of Secure*BPMN in practice in future [37].

The evaluation by the experts tested the perception of Secure*BPMN by an experienced audience. The evaluation by the MSc students tested how well an inexperienced, novice to IAS and BPMN, audience is able to learn and use Secure*BPMN after a one-hour training session.

All three parts of the experiment which are mentioned above are described in detail below.

- **Training Session on Secure*BPMN**

  A training session on Secure*BPMN, which was supported by the Microsoft Power Point slides, was given to the participants. The length of sessions vary between 45 minutes and 1 hour 30 minutes depending on how active the audience was and how many questions the presenter received. The same slides were used in all workshops and sent to the remote participants. The training explained the purpose of Secure*BPMN, its semantics, syntax and the application rules. The design rationale behind the symbols of the extension was also explained. One annotation example was presented to the participants. During training sessions, participants were allowed to ask question. No questions regarding Secure*BPMN were allowed during the remainder of the experiment.

- **Practical Tasks**

1. *Task 1 - Annotation*

   In Task 1, the participants were requested to security-annotate a BPMN diagram of a tender process using Secure*BPMN with the security details provided. The participants were presented with a BPMN diagram of a tender process accompanied by a text description of the process and of its security details. Each participant received a set of cut-out BPMN symbols/icons, scissors, glue and a pen. The participants were expected to cut-out Secure*BPMN shapes and stick them onto the BPMN diagram as they find appropriate. Alternatively, the participants were suggested to security-annotated the diagram using pens/pencils, if they find it easer than using cut-out shapes.

   The participants were given steps to follow while annotating the diagram using Secure*BPMN syntax. The Task 1 written material as received by the participants is presented in Appendix A.16. The scanned copies of the security-annotated diagrams collected from the participants in Task 1 are presented in Appendix A.21.

   In Task 1, the correct use of each Secure*BPMN variable (symbol), the correct use of the application rules and the general understanding of security-annotation technique were measured. The annotated diagrams were marked by the author according to the marking scheme which could be found in Appendix A.17.

   The correct use of each Secure*BPMN variable, namely Location, Access Permission, Information Format, Information Sensitivity, Security Goal, Criticality of Security Goal and Security Countermeasure, was tested twice. E.g. to test the correct usage of the attribute Location the participants were asked to mark the location of both Translate and supplier. The maximum score for each Secure*BPMN symbol was 2. The maximum score was allocated when a participant correctly used the variable in both cases.

   The maximum score of 2 was allocated for the correct use of the application rules if a participant applied Secure*BPMN according to the rules explained during a training session.

   To test the correct usage of Secure*BPMN variables the participants were prompted to represent information described in the task. The understanding of the diagram was tested via an ability of a participant to specify on a diagram his/her own knowledge. The participants were requested to depict at least one security goal and at least one security countermeasure at their discretion. One point was allocated for each variable.

   Tables 15-16 in Appendix A.23 present the marks allocated for the correctness of security-annotated diagrams resulted from Task 1.

2. *Task 2 - Interpretation*

   In Task 2, the participants, first, were presented with a BPMN diagram of a translation service provision process which was accompanied by a description. Then, the participants were presented with the BPMN diagram of the same process annotated with security information. There was no textual description of the security details of the process presented to the partic-

ipants. The annotated diagram was followed by a set of questions with regard to the security details of the process. The purpose of the questions was to establish how well the participants interpret Secure*BPMN annotations. The understanding and correct interpretation of each Secure*BPMN symbol was questioned twice. Some questions in Task 2 asked the participants to interpret symbols on the annotated diagram. Other questions were formulated to test the understanding of the meaning of annotations.

The score for each variable was allocated as follows: 0 - if both questions regarding the variable were answered incorrectly, 1- if only one question was answered correctly; and 2 - if both answers were answered correctly.

The written material used in Task 2 could be found in Appendix A.18. The correspondence between questions in the survey in Task 2 and Secure*BPMN variable and the marking scheme for Task 2 are presented in Appendix A.19. Tables 17-18 in Appendix A.23 present the marks allocated for the correctness in Task 2.

- **Post-task survey**

  The post-task survey, a copy of which could be found in Appendix A.20, was run online and consisted of three parts:

  1. *Collection of demographic data*

     The survey was anonymous and no personal identifiable details were collected. The respondents were questioned about their level of expertise in business processes in general, in BPMN and in IAS. For the level of expertise, each response was based on a 4-point Likert scale[14]:

     No knowledge | Some knowledge | Quite knowledgeable | Expert.

     The respondents also were questioned about their role in an organisation. They were prompted to describe the purpose for which they model business processes as well as to specify the area of their expertise in the IAS domain in case if they had any knowledge in the domain. The respondents location data were also collected.

  2. *Collection of the objective performance metrics*

     The participants self-reported the time which they spent on Tasks 1 and 2. In order to correspond an annotated-diagram (Task 1) with responses for Task 2 and post-task syrvey submitted online, each original BPMN diagram destined for annotation had a unique number which participants were requested to enter when answering the questions of the survey.

  3. *Collection of the subjective performance metrics*

[14]Likert scale is commonly used for measuring attitude in social sciences, medical and educational research. A Likert scale provides a range of answers or statements of agreement/disagreement from which a respondent may choose when answering a question [265].

In [37], the set of items (questions) is adopted, with the adjustment in wording, from the TAM [197] and used for the subjective evaluation of a modelling technique. The questions capture the opinion of a respondent with regard to the ease-of-use, usefulness and his/her intention to use a modelling techniques in future. In [167], a long procedure, which involved interviews with practitioners and score cards is used, to develop a set of questions for the evaluation of the ease-of-use, usefulness and intention to use BPMN.

In this thesis, the questions which are used in both [37] and [167] were analysed and re-formulated to fit the context of Secure*BPMN. Table 7.6 in this appendix summarises the analysis and shows the questions as they are adopted in this thesis. These questions were used in the post-task survey in order to capture the subjective metrics, namely Perceived Usefulness, Perceived Ease-of-Use and Intention to Use. In case if no appropriate question was found in other sources, a question was developed to capture the attitude of participants to a specific aspects critical for Secure*BPMN.

Column 2 of Table 7.6 shows the code of each question and in brackets the number under which this questions appeared in the post-task survey (Appendix A.20).

Five questions (PU1-PU5) on the post-task survey were used to operationalise Perceived Usefulness. Four questions (PEOU1 - PEOU4) on the post-task survey measured Perceived Ease of Use and three questions (ItU1-ItU3) measured Intention to Use. These 12 questions were combined and arranged in the questionnaire in a random order to avoid monotonous responses for questions covering the same construct. The answer to each question was measure using a 4-point Likert scale:

Strongly Disagree | Disagree | Agree | Strongly Agree

This is a "forced choice" scale. It has an even number of answers and omits the neutral (neither agree or disagree) option [266, 267]. The respondent were "forced" to choose whether they attitude towards Secure*BPMN is positive or negative.

It is not recommended to use a “forced choice" scale in a survey which concerns a highly sensitive topic where a respondent may prefer to choose a neutral option as an "opt-out". The survey carried out in this work did not cover a highly sensitive personal topic. Therefore, it was decided to exclude a neutral option for the following reasons. A neutral option may be interpreted by participants differently (e.g. "I am not sure", "I do not want to answer", "I do not care"). This would hinder the accuracy of results. A respondent may prefer to choose a neutral answer if he or she is unsure about the answer or use this option as an easy choice to avoid considering other options. For the analysis neutral answers provides little value.

The following weights were assigned to the options of the 4-point Likert scale in use: Strongly Disagree - 1; Disagree - 2; Agree - 4; Strongly Agree - 5. The mid-point of the measurement scale (3) is omitted in order to ensure that the distance between the answers is equal.

Tables 21-22 in Appendix A.23 present the collected survey answers.

Table 7.6: The questions for the collection of the perceived metrics

Construct	Question Code (No)	Questions in other sources	Questions as adopted in this thesis
Perceived usefulness	PU1 (Q24)	Overall, I find BPMN useful for modelling processes.[167, PU1]	Secure*BPMN is useful for the security annotation of business process models.
	PU2 (Q32)		Secure*BPMN provides a syntax for the modelling of all security concepts I require to visualise in business process models. (Ontological Completeness)
	PU3 (Q34)	Using this method would make it more difficult to maintain large data models [37, Q8]	Secure*BPMN would make security concerns in business process models easy to see and understand.
	PU4 (Q25)	Using this method would make it easier to communicate large data models to end users [37, Q13]	Secure*BPMN would facilitate communication with regard to security in business processes.
	PU5 (Q35)	Overall, I think this method does not provide an effective solution to the problem of representing [37, Q12]	Secure*BPMN provides an effective solution for representing security concerns in business process models.
Perceived ease of use	PEOU1 (Q26)	I find learning BPMN for process modeling is easy. [167, PEOU2] I found the method easy to learn [37, Q6]	Learning Secure*BPMN is easy.
	PEOU2 (Q33)	I found the rules of the method clear and easy to understand. [37, Q11]	The Secure*BPMN syntax (symbols, icons and applications rules) is intuitive, clear and easy to grasp. (Cognitive Effectiveness)
	PEOU3 (Q30)	I find creating process models using BPMN is easy. [167, PEOU3]	Using Secure*BPMN for annotating business process models with security details is easy.
	PEOU4 (Q27)	I am not confident that I am now competent to apply this method in practice [37, Q14]	I am now competent to apply Secure*BPMN in practice.
Intention to use	ItU1 (Q28)	If I retain access to BPMN, my intention would be to continue to use it for process modelling. [167]	In the future, if I am required to annotate business process models with security details, my intention would be to use Secure*BPMN.
	ItU2 (Q29)	I prefer to continue to use BPMN for process modelling over other process modeling grammars. [167, ItU3]	I prefer to continue to use Secure*BPMN for security annotation over other security extensions.
	ItU3 (Q31)		In the future, if I am required to gain a comprehensive vision of security issues in a business process, my intention would be to use Secure*BPMN.

7.3.3 Research Questions and Hypotheses for Testing

The success criteria were defined as a prerequisite for the experiment.

A group is considered to have coped with a task successfully if the following criteria regarding the objective metric *correctness score* are met:

1. The mean correctness score of a group is 70%[15] or above, and
2. The percentage of participants who scored below 30% (failed) is 5% or below[16].

A group considered to have perceived a quality of Secure*BPMN positively if the following criterion regarding a subjective metric is met:

The mean of a metric of a group is greater than the mid-point of a measurement scale[17].

The following research questions were formulated to be answered by the experiment:

RQ1 : *Are participants able to use Secure*BPMN successfully after a one-hour training session?*

RQ2 : *Does correctness score differ between experts and novices in each task?*

RQ3 : *Does the time required for the completion of each task differ between experts and novices?*

RQ4 : *Do correctness scores differ between Task 1 and Task 2 for each group?*

RQ5 : *Is there a correlation between the level of expertise and performance?*

RQ6 : *Do participants appraise the PEOU, PU and ItU of Secure*BPMN positively?*

RQ7 : *Does the perception of Secure*BPMN differ between experts and novices?*

These research questions were translated into the corresponding hypotheses to be statistically tested. The hypotheses are presented in Table 12 below (the corresponding alternative hypotheses are listed in Appendix A.22).

Table 7.7: Hypotheses for testing.

RQ	**Hypothesis**
RQ1	$H1.1_0$: The mean correctness score of all participants considered together in Task 1 is greater than 70% and the failure rate is below 5%.
RQ1	$H1.2_0$: The mean correctness score of all participants considered together in Task 2 is greater than 70% and the failure rate is below 5%.

Continued on the next page

[15]According to the generic grading criteria for written assessment [198], a score above 70% indicates an excellent pass and a score below 30% indicates a fail score.

[16]The choice of this threshold is further discussed in Section 7.3.4.2

[17]The following measurement scale was used in the experiment (with the corresponding weights assigned to the answers shown in brackets): Strongly Disagree (1); Disagree (2); Agree (4); Strongly Agree (5). The mid-point of the scale is 3. The scale and the justification of its choice could be found in Section 7.3.2

Table 7.7 – *Continued from the previous page*

RQ	**Hypothesis**
RQ1	$H1.3_0$: The mean correctness score of the group of experts in Task 1 is greater than 70% and the failure rate is below 5%.
RQ1	$H1.4_0$: The mean correctness score of the group of experts in Task 2 is greater than 70% and the failure rate is below 5%.
RQ1	$H1.5_0$: The mean correctness score of the group of MSc students in Task 1 is greater than 70% and the failure rate is below 5%.
RQ1	$H1.6_0$: The mean correctness score of the group of MSc students in Task 2 is greater than 70% and the failure rate is below 5%.
RQ2	$H2.1_0$: There is no difference between the correctness scores of the group of experts and MSc students in Task 1.
RQ2	$H2.2_0$: There is no difference between the correctness scores of the groups of experts and MSc students in Task 2.
RQ3	$H3.1_0$: There is no difference between the time the groups of experts and MSc students spent on Task 1.
RQ3	$H3.2_0$: There is no difference between the time the groups of experts and MSc students spent on Task 2.
RQ4	$H4.1_0$: There is no difference between the correctness scores of Task 1 and Task 2 for the group of experts.
RQ4	$H4.2_0$: There is no difference between the correctness scores of Task 1 and Task 2 for the group of MSc students.
RQ5	$H5.1_0$: There is a positive correlation between the level of expertise in IAS and performance.
RQ5	$H5.2_0$: There is a positive correlation between the level of expertise in BPMN and performance.
RQ6	$H6.1_0$: The mean of the PEOU construct of all participants considered together is greater than 3.
RQ6	$H6.2_0$: The mean of the PEOU construct of the group of experts is greater than 3.
RQ6	$H6.3_0$: The mean of the PEOU construct of the group of MSc students is greater than 3.
RQ6	$H6.4_0$: The mean of the PU construct of all participants considered together is greater than 3.
RQ6	$H6.5_0$: The mean of the PU construct of the group of experts is greater than 3.
RQ6	$H6.6_0$: The mean of the PU construct of the group of MSc students is greater than 3.

Continued on the next page

Table 7.7 – *Continued from the previous page*

RQ	Hypothesis
RQ6	$H6.7_0$: The mean of the ItU construct of all participants considered together is greater than 3.
RQ6	$H6.8_0$: The mean of the ItU construct of the group of experts is greater than 3.
RQ6	$H6.9_0$: The mean of the ItU construct of the group of MSc students is greater than 3.
RQ7	$H7.1_0$: There is no difference between the PEOU of the groups of experts and MSc students.
RQ7	$H7.2_0$: There is no difference between the PU of the groups of experts and MSc students.
RQ7	$H7.3_0$: There is no difference between the ItU of the groups of experts and MSc students.

7.3.4 Analysis of the Empirical Evaluation Results

7.3.4.1 Participants Profile

There were 31 individuals who participated in the empirical evaluation of Secure*BPMN. The profiles of the participants are summarised in Appendix A.23, Tables 13-14.

Among the participants there were 16 experts[18] who possessed experience in BPM, IAS or related domain, and 15 MSc students undertaking the Information Security & Privacy course at the School of Computer Science & Informatics, Cardiff University.

In the group of experts the IAS experience had a mean of 7 years and ranged from 1 to 25 years. The experience in BPMN, which ranged from 1 to 5 years, had 8 experts. Ten experts came from the UK, others were not originally from the UK, but at the time of the experiment studied towards PhD or worked in the UK. The level of expertise in IAS had a mean 2.9 on the scale of *1 (novice/no knowledge) - 2 (some knowledge) - 3 (quite knowledgeable) - 4 (expert)*. In this group there were 5 (31%) participants who described themselves as experts in IAS, 4 (25%) participants who identified themselves as quite knowledgeable about IAS and 7 (44%) possessed some knowledge in the IAS domain. The level of expertise in BPMN had a mean of 1.9 on

[18] In this experiment, any participant who had experience in either IAS or BPM or any related domain was assign to the group of experts as opposed to the group of MSc students which only included people who had no experience beyond an undergraduate education. The experts had either academic or industry background.

the same scale. Thus, the experts were quite knowledgeable about IAS, but had only a limited knowledge of BPMN. A wide range of different roles (managers, researchers, lecturers, consultant, business analyst etc.) and with experience in the diverse range of areas took part in the evaluation of Secure*BPMN. The group of experts participated in the evaluation experiment is representative of the prospective users of Secure*BPMN. Therefore, it is possible to generalise the results to the prospective audience of Secure*BPMN with a high degree of confidence.

The MSc students had no work experience and came to the MSc program straight after an undergraduate course. The MSc students had little or no knowledge of BPMN. However, the group of MSc students received a 30 minutes introduction to BPMN and its basic shapes prior to the experiment. The group was also familiar with UML activity diagram. At the time of the experiment, the MSc students started, but not completed several IAS modules. Hence, this audience allows testing how well Secure*BPMN is understood and how well it is exploited by users who are not highly experienced in BPMN.

7.3.4.2 Objective Performance Metrics (*H1.1 - H1.6*)

Two objective performance metrics, time and correctness, are analysed in this section and hypotheses *H1.1 - H1.6* are tested.

The scanned copies of the security-annotated diagrams collected from the participants in Task 1 are presented in Appendix A.21. Tables 15-16 in Appendix A.23 present the correctness marks for Task 1. Tables 17-18 in Appendix A.23 present the correctness marks for Task 2. Section 7.3.2 explains how the responses were marked. The marking schemes are described in Appendix A.17 and A.19 for Tasks 1 and 2 respectively.

Table 19 in Appendix A.23 shows the summary of the performance metrics for all participants for both tasks. The descriptive statistics for both tasks and for both groups as well as the overall average are presented in Table 7.8 of this section.

The box-and-whisker plot in Figure 7.6 shows the central tendency, the variability of the correctness scores and the outliers. The box-and-whisker plot in Figure 7.7 shows the central tendency, the variability of the tasks' completion time and the outliers.

The comparison of the means of correctness scores of two tasks for all participants shows that the interpretation task (Task 2) was performed better than the annotation task (Task 1). Task 1 was completed with the average correctness score of 74.35±16.92%, while Task 2 with the correctness of 76.73±19.95%. However, the situation is not uniformed across the groups. The experts completed the interpretation task better than the annotation task (the mean score is 77.57±16.83% for Task 1 and 84.82±14.73% for Task 2). The MSc students, in contrast, performed the annotation task better than the interpretation task (the average score is 70.91±16.90% for Task 1 and 68.10±21.58% for Task 2).

Table 7.8: Descriptive statistics for objective performance metrics

Statistics	Time		Correctness Score			
	Task 1 (mins)	Task 2 (mins)	Task 1 (out of 18)	Task 1 (%)	Task 2 (out of 14)	Task 2 (%)
Experts (N=16)						
Min	13.00	3.00	8.00	44.44	8.00	57.14
Max	45.00	24.00	17.90	99.44	14.00	100.00
Mean	20.81	9.44	13.96	77.57	11.88	84.82
Standard dev.	9.58	5.72	3.03	16.83	2.06	14.73
MSc students (N=15)						
Min	25.00	3.00	7.75	43.06	1.00	7.14
Max	60.00	15.00	16.75	93.06	13.00	92.86
Mean	38.80	8.80	12.76	70.91	9.53	68.10*
Standard dev.	8.68	3.14	3.04	16.90	3.02	21.58
All participants (N=31)						
Min	13.00	3.00	7.75	43.06	1.00	7.14
Max	60.00	24.00	17.90	99.44	14.00	100.00
Mean	29.52	9.13	13.38	74.35	10.74	76.73
Standard dev.	12.83	4.59	3.05	16.92	2.79	19.95
* - the score below the success level of 70%.						

While the experts scored in Task 2 on average 11.88±2.06 out of 14 (84.82±14.73%), the MSc students scored only 9.53±3.02 out of 14 (68.10±21.58%).

While the annotation task (Task 1) was completed by the experts faster and with a higher score than the MSc students, the situation in Task 2 is different (Table 7.8). The experts completed the interpretation task (Task 2) also with the score higher than the MSc students, but it took them longer than the students to complete the task. Although the experts spent more time on interpreting the diagram, they interpreted it more accurately than the MSc students.

Table 7.8 confirms that the mean score for all participants and for the group of experts for both tasks is above 70%. In the group of MSc students, the mean correctness score in Task 1 is also above 70%. However, in Task 2 the mean score of the MSc group is 1.9% below the success score of 70%.

Table 7.9 shows the number of participants in the various score ranges. In Task 1 no participants failed, but at the same time no participants received the maximum possible mark. Eighteen participants completed Task 2 with the score in the range 70-99% and 13 participants passed with the score in the range 30-69%. In Task 2, five participants (all experts) answered all questions correctly and received the maximum score. Only one MSc student failed in Task 2 taking the group failure rate up to 6.67%. Nineteen participants

Figure 7.6: The distribution of correctness scores

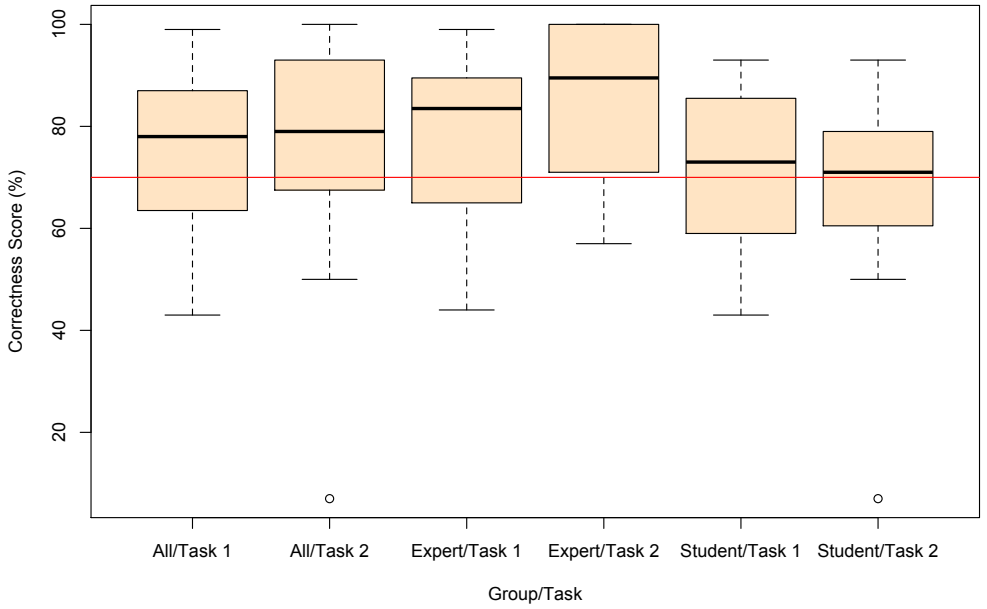
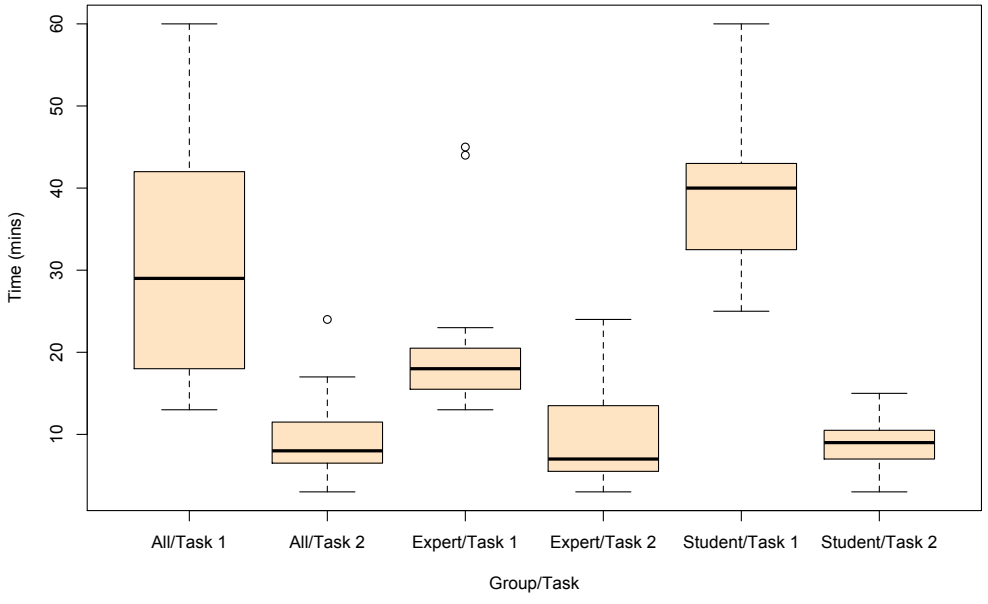


Figure 7.7: The distribution of time



completed Task 2 with the score in the range 70-99% and 7 participants with the score in the range 30-69%. Table 7.9 also indicates that in terms of the number of participants in each score range both tasks were performed by the experts better than by the MSc students. Table 7.9 and Figure 7.6 also show that at least over 53.33% of participants in each group completed the tasks with the individual score above the success

score of 70%.

Table 7.9: Count and percentage of the participants grouped by correctness score range.

Score Classification		All (N=31)		Experts (N=16)		MSc Students (N=15)	
Score Range	Equivalent [198]	Task 1	Task 2	Task 1	Task 2	Task 1	Task 2
100	Exceptional Pass	0 (0.00%)	5 (16.13%)	0 (0.00%)	5 (31.25%)	0 (0.00%)	0 (0.00%)
70-99	Excellent Pass	18 (58.06%)	19 (61.29%)	10 (62.50%)	9 (56.25%)	8 (53.33%)	9 (60.00%)
30-69	Pass	13 (41.94%)	7 (22.58%)	6 (37.50%)	2 (12.50%)	7 (46.67%)	5 (33.33%)
below 30	Fail	0 (0.00%)	1 (3.23%)*	0 (0.00%)	0 (0.00%)	0 (0.00%)	1 (6.67%)*
* - the failure rate is above 5%.							

Table 7.10 provides a summary on testing hypotheses *H1.1 - H1.6* and shows that *H1.6* is rejected because none of the success criteria was met, while *H1.1-H1.5* are accepted because both success criteria were satisfied (i.e. only the group of MSc students failed to complete Task 2 successfully, while the group of experts and all participants considered together completed both tasks successfully as well as did the MSc students in Task 1).

Table 7.10: Summary of testing hypotheses H 1.1 - H 1.6

Success Criteria/Group	All (N=31)		Experts (N=16)		MSc Students (N=15)	
Hypothesis	*H1.1*	*H1.2*	*H1.3*	*H1.4*	*H1.5*	*H1.6*
Mean Score≥70%	YES	YES	YES	YES	YES	NO
Fail Percentage≤5%	YES	YES	YES	YES	YES	NO
Success	YES	YES	YES	YES	YES	NO

When considering this failure of the MSc group to complete Task 2 successfully, it must be accounted for the fact that the success criteria chosen are ,strict particularly with regard to the failure rate. The failure rate of 5% was set to be suitable for groups of various sizes. For example for a group of 100 participants, the success failure rate of 5% means that the group is successful if less than 5 participants failed. However, for the group of a smaller size such as in this experiment 5% failure rate means that no student is allowed to fail for the group to succeed.

For investigating the reasons of the unsuccessful performance of the MSc students in Task 2, the boxplot in Figure 7.6 is useful. It shows that there is an outlier in Task 2. It is *Participant 18*, who scored only 7.14% in Task 2. In Task 1, however, *Participant 18* scored 73.06%. This shows that the participant got understanding of Secure*BPMN sufficient for the successful fulfilment of the annotation task. It is worth

noting though that on the completion of Task 1 *Participant 18* spent 60 minutes, which is longer than anyone else spent on the completion of Task 1. On Task 2, *Participant 18* spent only 10 minutes which is close to the mean time in Task 2. It is possible to suggest that either the MSc student did not have sufficient time for interpreting the security-annotated diagram in Task 2 and rushed through the questions ticking up the answers randomly, or simply did not put enough effort into the task. If the result of *Participant 18* (outlier) is excluded from the MSc group results in Task 2, than the mean score of the MSc group in Task 2 raises up to 72.45% and the failure rate drops down to zero. Hence, the exclusion of Participant 18 enables the group of MSc students to satisfies the success criteria confidently. Thus, although the group of MSc students failed to complete Task 2 successfully, the score and failure rate of the group are only insignificantly below the success criteria. Furthermore, the results do not meet the success criteria due to the poor performance of one particular participant, rather than due to a consistently low performance of the whole group.

7.3.4.3 Correlation Between Objective Performance Metrics in groups (*H2.1, H2.2, H3.1* and *H3.2*)

In order to choose the right test for verifying hypotheses *H2.1, H2.2, H3.1* and *H3.2*, first, the normality of the distribution of all four objective metrics for each group was checked with the Shapiro-Wilk test and, second, the homogeneity of the variance between the same metric of two groups was checked with the Levene's test. These tests are typically used to support the choice of a test to verify if the distribution of populations is identical. The experiment had observation independence by design because the participants worked independently. The results returned by the tests are summarised in Table 20 in Appendix A.23. Based on these results, the ANOVA test was chosen to test *H2.1*, because the samples satisfy the requirements of the ANOVA test (observation independence, the homogeneity of variance and normality of distribution). The Mann-Whitney-Wilcoxon test was chosen to test the other hypotheses, because at least one sample was not confirmed to be normal and the Mann-Whitney-Wilcoxon test allows testing if the distribution of populations is identical without assuming them to follow a normal distribution. The results of the tests are presented in Figures 38-40 in Appendix A.23 and are discussed below.

On average, the MSc students spent more time on the annotation task (Task 1) than the experts (38.80±8.68 and 20.81±9.58 minutes respectively). It was expected that the novice audience would spend more time on the completion of the tasks. This expectation was confirmed in Task 1. The statistical analysis of the experimental data indicates that the difference between the time the MSc students and experts spent on the completion of Task 1 is statistically significant (*H3.1*: p-value<0.05 (Figure 39 in Appendix A.23)).

However, while the analysis of the time spent on Task 1 supports the assumption that experts are able to complete a task faster, the analysis of the time spent on Task 2 rendered different result. While the experts spent on average 9.44±5.72 minutes on the interpretation task (Task 2), the MSc students spent only 8.33±3.14 minutes. The statistical analysis though shows that although the MSc students spent less time

on Task 2 than the experts, the difference is not statistically significant (*H3.2*: p-value>0.05 (Figure 39 in Appendix A.23)).

While the experts scored on average 77.57±16.83% in annotation task, the MSc students scored only 70.91±16.90%. Although the experts performed Task 1 with higher score, the ANOVA test indicates that the difference is not statistically significant (*H2.1*: p-value>0.05 (Figure 38 in Appendix A.23)). This means that even a novice audience is capable of using Secure*BPMN for security-annotations at the level of correctness which is not significantly lower than the correctness of a more experienced audience taking into account that it takes a novice audience longer to complete the task.

In Task 2, where the experts on average also scored higher than the MSc students (84.82± 14.73% and 68.10±21.58% for the experts and students respectively), the difference is statistically significant (*H2.2*: p-value<0.05 (Figure 38 in Appendix A.23)). The MSc students scored significantly lower on the interpretation task, hence they require more training and practice on the interpretation of security-annotated diagrams.

While the experts demonstrated consistent scores in both tasks (*H4.1*:p-value>0.05), the MSc students scored in Task 1 higher than in Task 2 with statistical significance (*H4.2*: p-value<0.05 (Figure 40 in Appendix A.23)).

7.3.4.4 Correlation Between the Level of Expertise and Performance (*H5.1* and *H5.2*)

For the group of experts, the correlation between experience and performance was also examined. For this purpose, the Pearson product moment correlation coefficient (R)[19] was analysed.

In Task 1, a moderate positive correlation exists between the level of expertise in the IAS domain and the correctness of the task performance with R equal 0.42. In Task 2, a weak positive correlation is encountered between the level of expertise in the IAS domain and the correctness results with R equal 0.36. Hence, the experts who are more experienced in IAS scored in both tasks higher than their less experienced colleagues. However, the correlation as not linear as reflected by the correlation coefficient.

There is a weak negative correlation between the level of expertise in IAS and the time the experts spent on Task 1 (R=-0.34). In Task 2, a more significant moderate negative correlation is observed with R equal

[19]The Pearson product moment correlation coefficient (R) measures the strength of a correlation [199]. The magnitude of R in this thesis is interpreted according to the following scale [200]: 0.8 to 1.0 or -0.8 to -1.0 (very strong relationship); 0.6 to 0.8 - strong relationship; 0.4 to 0.6 - moderate relationship; 0.2 to 0.4 - weak relationship; 0 to 0.2 - weak or no relationship. However, it is worth noting that the interpretation of R vary in different research.

-0.54. Thus, more experienced in IAS participants performed both tasks faster and with the higher level of correctness.

In Task 1, a weak positive correlation is observed between the level of experience in BPMN and the correctness of task performance with R equal 0.32. This type of correlation is confirmed in Task 2 with even greater R equal 0.56 indicating a moderate correlation. Again the participants who had higher level of expertise in BPMN performed better in both tasks.

Both hypotheses *H5.1* and *H5.2* were corroborated by the experiment.

7.3.4.5 Examination of Survey Results

Twelve items (questions) on the post task survey, which is presented in Appendix A.20, examined the attitude of the participant regarding three subjective metrics: Perceived Ease of Use (PEOU), Perceived Usefulness (PU) and Intention to Use (ItU). These twelve questions are summarised in Table 7.6. Tables 21-22 in Appendix A.23 present the collected survey answers.

The constructs validity and reliability analysis was conducted and confirmed the acceptable level of the reliability of the survey data (excluding item PEOU4). The reliability analysis is presented in Appendix A.24.

Figure 7.8 below summarises the survey answers collected and shows the mean score for each item of the survey for all participants considered together. Figure 7.8 indicates that the questions PEOU1[20] and PEOU2[21] received the highest score of 4.23. These numbers confirm that, according to the post task survey, the participants after using Secure*BPMN found it to be an easy-to-learn notation and regarded its syntax as clear and intuitive. These results support the hypothesis about the cognitive effectiveness of the Secure*BPMN syntax. The lowest score was received by the item ItU2[22]. As it was established during the evaluation workshops, the majority of the participants were not familiar with other security-annotation techniques and, therefore, did not actively express their preference towards Secure*BPMN over other security-annotation techniques. The item PU2[23] received a low score of 3.39, which means that the participants did not perceive Secure*BPMN to be complete to the level they perceived it to be easy-to-learn and clear.

Figure 7.9 also summarises the responses of the participants for each question and shows the number of participants by answers provided. The y-axis shows the code of the question in the post-task survey as

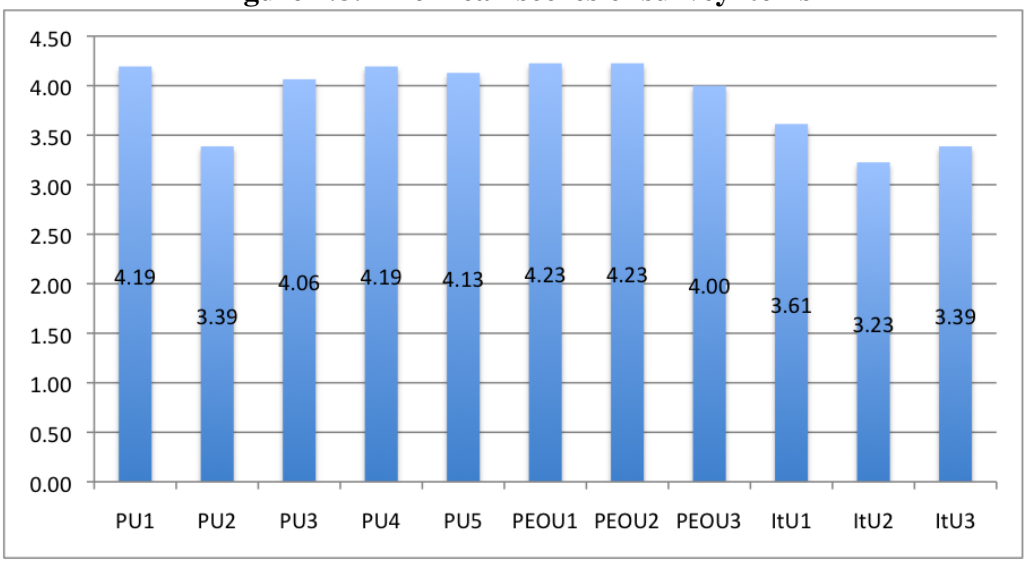
[20]PEOU1 - Learning Secure*BPMN is easy (Table 7.6).

[21]PEOU2 - The Secure*BPMN syntax (symbols, icons and applications rules) is intuitive, clear and easy to grasp

[22]ItU2 - I prefer to continue to use Secure*BPMN for security annotation over other security extensions

[23]PU2 - Secure*BPMN provides a syntax for the modelling of all security concepts I require to visualise in business process models.

Figure 7.8: The mean scores of survey items



outlined in Table 7.6 and the x-axis shows the number of the responses. Tables 26, 25 and 24 in Appendix A.23 present the supporting data for Figure 7.9.

Figure 7.9 shows that in none of the questions Secure*BPMN received a strongly negative evaluation. The largest number of participants (12) *strongly agreed* with the statements that Secure*BPMN is useful for the security-annotation of business process models and may facilitate communication with regard to security (items PU1 and PU4).

The largest number of the participants (24) *agreed* that Secure*BPMN provides an effective solution for representing security concerns in business process models (item PU5).

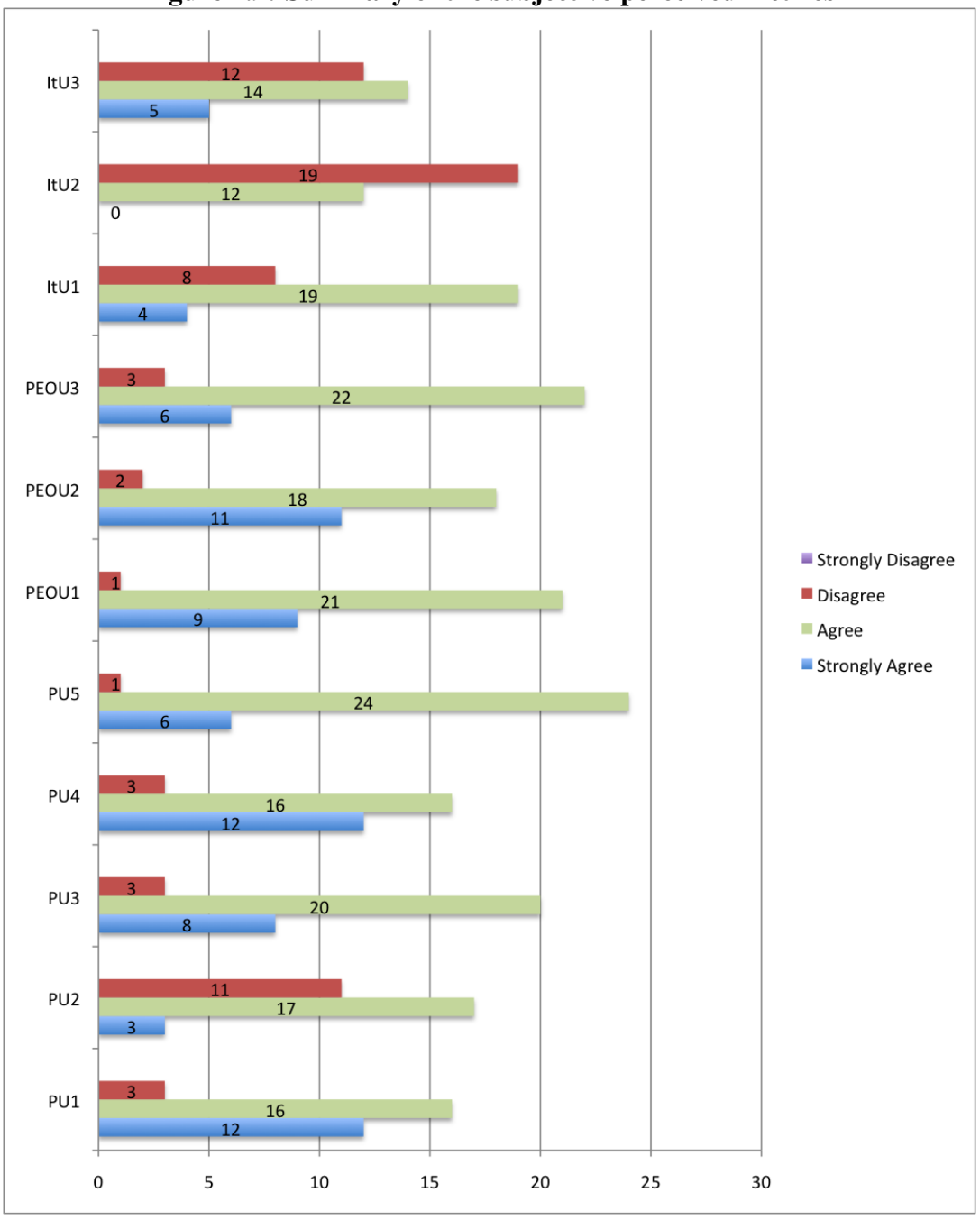
The largest number of participants (19) *disagreed* with the statement ItU2 - "*I prefer to continue to use Secure*BPMN for security annotation over other security extensions*". The statements ItU3 -"*In the future, if I am required to gain a comprehensive vision of security issues in a business process, my intention would be to use Secure*BPMN*" also received a large number of responses with disagreement (12).

The statement PU2 - "*Secure*BPMN provides a syntax for the modelling of all security concepts I require to visualise in business process models.*" also received a large number of responses with *disagreement* (11). It means that 11 out of 31 participants cast doubts upon the completeness of the semantics of Secure*BPMN. Among these 11 participants there were 6 experts and 5 MSc students.

7.3.4.6 Subjective Perceived Metrics (*H6.1-H6.9* and *H7.1-H7.3*)

Table 23 in Appendix A.23 shows the score of each constructs for each participant. Table 7.11 below summarises the survey results for the three constructs PU, PEOU and ItU for the groups of MSc students

Figure 7.9: Summary of the subjective perceived metrics



and experts, and shows the overall means as well. For all three constructs the score shown is the score out of 5.

Table 7.11: Subjective performance metrics. Means.

Group/Construct	**PU**	**PEOU**	**ItU**
Experts	4.06	4.15	3.50
MSc students	3.92	4.16	3.31
Overall	3.99	4.15	3.41

Table 7.11 confirms that the means of all metrics for both groups as well as the overall means are above the mid-point of the measurement scale (3).

In order to test hypotheses *H6.1-H6.9* statistically, one sample t-tests (one-tailed) were run with the perceived metrics (the full output of the tests is presented in Figure 41 in Appendix A.23). The results of the hypotheses *H6.1-H6.9* testing are discussed below.

Hypotheses *H6.1-H6.8* are rejected (p-values<0.05 (Figure 41 in Appendix A.23)). This means that the means of POEU and PU constructs of the groups experts and MSc students as well as of all participants together are greater than 3 with statistical significance.

For the ItU construct while the null hypothesis is rejected for all participants considered together and for the group of expert (p-value<0.05), it is tentatively accepted for the group of MSc students because p-value although greater than 0.05, but only insignificantly (p-value=0.056) (Figure 41 in Appendix A.23). This implies that the mean of ItU for all participants and the experts is greater that 3 and the difference is statistically significant. The mean of ItU of the MSc students is greater than 3, but the difference is not statistically significant.

Table 7.11 shows that Secure*BPMN was perceived by the MSc students to be slightly easer to learn and to use (PEOU=4.16) than it was perceived by the experts (PEOU=4.15). In [37], for example, it is hypothesised that experts would usually find learning a new method easier than novices. Nevertheless, with Secure*BPMN the novice participants found the method easier to use than more experienced participants.

At the same time, the experts perceived Secure*BPMN as more useful (PU=4.06) and expressed a higher level of the intention to use Secure*BPMN in future (ItU=3.50) than the MSc students (PU=3.92 and ItU=3.31).

The largest difference in the evaluation between the groups of experts and MSc students was regarding their Intention to Use Secure*BPMN. While the MSc students were more careful with expressing their intention to use Secure*BPMN (ItU=3.31), the group of experts demonstrated stronger intention to use Secure*BPMN in future (ItU=3.50).

Within each group the PEOU construct scored the highest, with the PU and ItU constructs taking the second and third places respectively (this coincides with the trend observed in [37]). This implies that the

participants found Secure*BPMN to be easy-to-use with a higher level of confidence than they found it to be useful. The lowest overall score was received by the ItU construct (ItU=3.41). Such a low score may be explained by the following considerations. First, not every participant models secure business process as a part of his/her job. Therefore, there may be no need and no opportunity for some participants to use Secure*BPMN in future. Another reason is that many participants were not familiar with other security-annotation techniques and were reluctant to agree to use Secure*BPMN over other security-annotation techniques before exploring alternative methods.

In order to test the difference in perception of Secure*BPMN between the experts and MSc students statistically (hypotheses *H7.1-H7.3*), the Mann-Whitney-Wilcoxon test was used. The full output of the tests is presented in Figure 42 in Appendix A.23. The results of the hypotheses *H7.1-H7.3* testing confirm that all three perceived metrics received relatively close evaluation by the groups of experts and MSc students. All three hypotheses *H7.1-H7.3* are accepted since all returned p-values are greater than 0.05. This means that there was no statistically significant difference between the perception of the experts and MSc students for any of the three perceived metrics.

7.4 Discussion of the Evaluation Results

First, this section discusses the results of the analytical and empirical evaluation conducted. Then, it outlines the limitations of the evaluation process and threats to the validity of the evaluation results.

7.4.1 Analytical Evaluation Results

The last row of Tables 5.3, 5.4, 5.5 and 5.6 presents Secure*BPMN for the comparison purposes. The references to the above mentioned tables are made further in this section.

The representational analysis confirmed that Secure*BPMN is ontologically complete and clear to the degree it is possible in the context of a BPMN extension. Secure*BPMN exhibits a higher degree of ontological completeness than any other examined security extension as discussed in Section 7.2.1. According to the representation model [191], this implies that Secure*BPMN has a higher expressive power than other extensions.

Table 5.3 indicates that no other extension, apart from Secure*BPMN, considers a wide range of experts with different backgrounds. The focus of Secure*BPMN on humans rather than machines called for a thoroughly elaborated syntax with a well-grounded cognitive effectiveness. Secure*BPMN was developed primarily for human comprehension and was evaluated in order to show that it fulfils this purpose, rather than showing its suitability for automatic processing and execution.

Table 5.3 also confirms that among the extensions analysed only two proposals apart from Secure*BPMN used the TVND to guide the development of their syntax. However, as already discussed in Section 5.4.3, the details of the use of the TVND there is very scarce.

The syntax of Secure*BPMN, in contrast to other extensions, is thoroughly examined in terms of the nine principles of the TVND. The syntactical analysis in Section 7.2.2 confirms that Secure*BPMN takes into account all principals of the TVND. All trade-offs made during the syntax design are carefully documented and justified. The syntactical analysis demonstrates that a special effort was put to ensure the cognitive effectiveness of Secure*BPMN syntax and, therefore, based on the TVND it may be predicted that the syntax of Secure*BPMN is cognitively effective.

7.4.2 Empirical Evaluation Results

This section sums up the answers to the research questions posed for testing in Section 7.3.3.

RQ1: *Are participants able to use Secure*BPMN successfully after a one-hour training session?*

Answering this question was the major objective of this evaluation experiment. The experiment confirmed that all participants when considered together and the group of experts coped with both practical tasks successfully, i.e. the mean correctness score of a group was above 70% and the failure rate was below 5%. They were able to use Secure*BPMN for both annotation and interpretation correctly after a one-hour training session on the security-annotation technique. The group of MSc students completed the annotation task successfully, but did not meet the success criteria in the interpretation task. As discussed in Section 7.3.4.2, such result stems from the poor performance of one MSc student who failed to complete the interpretation task and if the performance result of this student is excluded from the analysis then the MSc group satisfies the success criteria.

The empirical evaluation corroborated that the participants who are more experienced either in BPMN or IAS were able to use Secure*BPMN more successfully. These results were predictable. However, what is more important in the context of this thesis, the evaluation experiment also confirmed that even a non-experienced audience was able to learn and to use Secure*BPMN successfully for the annotation of BPMN diagram. It is also worth noting that although the group of MSc students did not perform successfully in the interpretation task, the mean score gained by the group was only 1.9% lower than the success score and over a half of the group completed the task with an individual score greater than 70%.

Hence, with an improvement of the training material even an audience novice to BPMN and IAS may be able to complete both tasks with the mean score above 70%. The experiment confirmed that the less experienced prospective users of Secure*BPMN require more detailed training on the interpretation of security-annotated diagrams and required to see a larger number of annotated examples. It must be noted here that

during the training session on Secure*BPMN only an annotation example was given and the interpretation of a security-annotated diagram was not exemplified.

The results of the evaluation and, more specifically, the results regarding the common errors with Secure*BPMN annotations, enable the improvement of a training session on Secure*BPMN. In future, more attention during a training must be paid to the importance of obeying the grammar rules of Secure*BPMN, i.e. the correct positioning of Secure*BPMN symbols and the use of the correct type of a security association line. The possibility of attaching Secure*BPMN elements to a wide range of BPMN elements, as permitted by Secure*BPMN compositional rules, must be made clear to participants.

RQ2: *Does correctness score differ between experts and novices in each task?*

The group of experts scored in both tasks higher than the group of MSc. However, while in the annotation task the difference between the mean scores of the groups was not statistically significant, in the interpretation task it was. These results indicated that more experienced users are capable of using Secure*BPMN more efficiently. However, the results also evidenced that even a novice audience is able to use Secure*BPMN successfully for annotation.

RQ3: *Does the time required for the completion of each task differ between experts and novices?*

The experts completed the annotation task faster than the MSc students with statistical significance. This outcome was predictable and expected. The interpretation task, however, the MSc students completed faster, but the difference in time was not statistically significant and it is worth noting that the MSc students scored significantly lower than the experts in this task. On the one hand, it may be suggested that the MSc students possibly had no sufficient knowledge to complete this task. On the other hand, the results with high probability indicate that the students rushed through the interpretation task at the expense of correctness score.

RQ4: *Do correctness scores differ between Task 1 and Task 2 for each group?*

The experts demonstrated consistently high performance in both tasks. The MSc students performed the annotation task better than the interpretation task with statistical significance. It was expected that the groups will demonstrate consistent results in both tasks. Therefore, the result indicates that there is a problem with the performance of the MSc students in Task 2 and it, as already discussed earlier in this chapter, relates to the failure of one MSc student to complete the task.

RQ5: *Is there a correlation between the level of expertise and performance?*

The empirical evaluation demonstrated that the participants who are more experienced either in BPMN or IAS were able to use Secure*BPMN more successfully since there was a weak to moderate correlation observed between the levels of experience and correctness scores.

The group of experts which coped successfully with both tasks consisted of experts with different backgrounds, not necessarily technical or security-focused. This implies that Secure*BPMN may be learnt and

successfully utilised by experts irrespective of their background and specialisation.

RQ6: *Do the participants appraise the PEOU, PU and ItU of Secure*BPMN positively?*

The statistical tests confirmed that both groups as well as all participants together apprised the PEOU and PU of Secure*BPMN at the level which is higher than the mid-point of the measurement scale with statistical significance. For the ItU construct the same situation was observed for the group of experts and for all participants together. Only the group of MSc students appraised the ItU construct although at the level greater than the mid-point of the measurement scale, but not statistically significantly greater. The results of the statistical analysis of the post-task survey confirmed that the participants perceive Secure*BPMN as an easy-to-use and useful notation. The participants express the intention to use Secure*BPMN in future. However, the confidence of the participants regarding the ease-of-use and usefulness of Secure*BPMN was higher than their confidence regarding their future use of the proposed technique. The possible reasons for this attitude are discussed in Section 7.3.4.6.

According to the MEM [37], it is possible to predict that Secure*BPMN has a potential to be adopted in practice because all three subjective perceived metrics (PEOU, PU and ITU) were perceived positively by the participants (i.e the mean scores of the perceived metrics were above the mid-point of the measurement scale).

RQ7: *Does the perception of Secure*BPMN differ between experts and novices?*

Although there was a difference between the perception of Secure*BPMN by experts and MSc students in this experiment, the difference was not statistically significant. Hence, this experiment additionally confirmed that in the future experiments MSc students may stand proxies for experts while the latter may not be employed due to various reasons.

7.4.3 Threats to Validity

The major limitation of the analytical evaluation is that it was conducted by the extension developer who is inevitably biased toward the extension. Addressing this concern, a well-established evaluation frameworks were used for the analytical evaluation and the rules of the frameworks were obeyed to guarantee the trustworthiness and plausibility of the evaluation outcomes. Additionally, an empirical evaluation of the proposed annotation technique with prospective users, who were impartial to Secure*BPMN, was undertaken to complement the analytical evaluation. In order to avoid bias in analysis the results of both analytical and empirical evaluation were thoroughly documented.

While discussing the outcomes of the empirical evaluation experiment, the following threats to the validity must be accounted for.

A sample of the participants evaluating Secure*BPMN was small, Therefore, the result of the statistical tests must be considered with caution. To make more precise predictions regarding the adoption of Secure*BPMN in practice in future more experiments with a larger number of participants are required.

While the group of MSc students was homogeneous as they all had the same level of knowledge and work experience, the group of experts was not heterogeneous because the level of expertise and background varied noticeably among the experts. However, the main reason for choosing such a diverse group of experts was to demonstrate that experts with various backgrounds and levels of expertise may successfully use Secure*BPMN.

The time spent by the participants on the annotation and interpretation of diagrams was self-reported by the participants. This is a potential source of error since the precision of this information was not feasible to monitor.

The behaviour of the participants affected the results of the experiment. The participants who were present at the workshops had only limited time to complete the tasks. It may be inferred from the analysis of the diagrams annotated by the MSc students that they rushed to complete the annotation exercise and did not depict any additional security countermeasures that were the last on the list of the instruction the participants were asked to follow. Although this inference is made with caution because the students possibly were just not experienced enough in IAS to complete the exercise.

Although the participants were requested to work independently, the plagiarism was observed in two annotated diagrams in the group of MSc students. Two participants who were sat together while security-annotating diagrams replicated the same error.

The nature of the experiment was non-comparative due to two reasons. First, there are no other security-annotation technique that would fulfil the same purposes as Secure*BPMN and have a similar semantics which could be used for the comparison. Also the author is not aware about any other security-annotation extension for BPMN being evaluated using the MEM. There was no data available regarding the effectiveness of other security-annotation methods for BPMN to benchmark Secure*BPMN against in terms of objective and subjective metrics. Second, the organisation of a comparative experiment is hard within the scope of a PhD thesis (cf. [201, 202]). It is complicated, among other factors, by the limited availability of participants and their low motivation. It is worth noting that the participants of the experiment in this research spent their time voluntary with no reward. Hence, the objective and subjective metrics received during the evaluation experiment were only analysed in respect to the predefined success criteria and compared between the groups of experts and novices, and were not compared with the similar metrics of other security-annotation techniques.

7.5 Chapter Summary

In this chapter, Secure*BPMN is evaluated in order to achieve Objective 2.A (Section 1.3). The purpose of the evaluation was to test Hypothesis A, which is formulated as follows: *Secure*BPMN is an ontologically complete and cognitively effective modelling notation which is perceived by experts with different backgrounds and with the different levels of experience in IAS and BPM as a useful and easy-to-use modelling technique which is likely to be adopted in practice* (Section 1.4).

The hypothesis was confirmed by the analytical and empirical evaluations. It was demonstrated that Secure*BPMN exhibits greater ontological completeness than other examined BPMN security extensions. The cognitive effectiveness of Secure*BPMN was achieved by obeying the principles of the TVND, the conformance to which was examined in this chapter. The empirical evaluation corroborated that prospective users perceive Secure*BPMN, after using it in two practical tasks, as an easy-to-use, easy-to-learn and useful security-annotation technique which has a potential to be adopted in practice.

Finally, this section revisits the drawbacks of other security extensions summarised in Section 5.5 and explains how Secure*BPMN addresses them:

- *The semantics of the extensions examined is weakly justified and suffers from granularity, inconsistency and incompleteness*.

  The justification of the semantics of Secure*BPMN is grounded in the thorough multi-phase evaluation of the RMIAS. The RMIAS, as proved in Chapter 4, reflects a commonly agreed understanding of the IAS domain. The security constructs which were introduced into BPMN were consistently extracted from the RMIAS, the process was carefully documented and all inclusion/exclusion decisions were justified (Section 6.1).

  The comprehensiveness of the semantics of Secure*BPMN comes from the RMIAS. Secure*BPMN enables simultaneous modelling of all security concepts of the RMIAS, namely security goals, security countermeasures, the characteristics of information and access permissions. Taking into account the wide-spread of collaborative business processes, Secure*BPMN permits modelling of access permissions at an inter-organisational level which is not possible in any other extension examined.

- *The semantics of the extensions does not reflect an holistic approach to IAS.*

  Secure*BPMN inherits an holistic approach to IAS from the RMIAS. The holistic approach in Secure*BPMN is revealed via the ability to represent the security countermeasures of all four types, which are distinguished in the RMIAS (legal, human-oriented, organisational and technical).An holistic approach to IAS in Secure*BPMN is also stems from the perception of the purposes of business processes to be diverse and not limited to the facilitation of code generation. Appendix A.15 provides more detailed discussion on this.

- *The syntax of the extensions is paid little attention and lacks cognitive effectiveness.*

In this thesis, significant time and effort was devoted to the design of the cognitively effective syntax for Secure*BPMN. The principles of the TVND, which was used as a guidance, were followed. All design decisions were documented and explained as well as all trade-offs which are inevitable in the syntax design process. The careful documentation of the syntax design decisions makes them traceable, easy to analyse and evaluate.

- *The absence of the detailed evaluation of the syntax, semantics and overall effectiveness of the extensions examined.*

  Table 5.4 confirms that this thesis conducts more extensive and detailed evaluation of the proposed modelling technique than any of the papers examined in Chapter 5. In this thesis, Secure*BPMN was evaluated both analytically and empirically. The analytical evaluation, which was based on widely accepted in the current literature evaluation frameworks, addressed the ontological completeness of the semantics and the cognitive effectiveness of the syntax of Secure*BPMN. The empirical evaluation was also based on a widely used evaluation framework - the MEM. The ease-of-use, usefulness and the intention to use Secure*BPMN as expressed by prospective users after a training session and practical exercise with Secure*BPMN were tested using the MEM.

The following final chapter of this thesis summarises the contribution of the thesis and discusses the future work.

Chapter 8

Conclusions

This chapter reviews the work presented in the preceding chapters. First, the achievement of the research objectives and the confirmation of the hypotheses are discussed. This chapter also outlines future work that may stem from this research project and concludes with the discussion of the originality and significance of the research presented.

8.1 Achievement of the Research Objectives

Two research objectives with two sub-objectives each were identified in Section 1.3. The degree to which these objectives are achieved along with the methods used are discussed below. The major objective of the thesis was to design a graphical modelling language to enable weaving security into business process models, since a modelling language requires a semantics the discussion of the objectives stars with the development of the basis for the semantics.

Objective 1.B: *Develop a comprehensive conceptual model of the IAS domain which represents the domain in its contemporary state and in the form suitable for a multi-disciplinary group of experts such that this model may serve as the basis for the semantics of a modelling technique.*

The initial analysis of the existing security-modelling languages revealed that they have different semantics and that their semantics is typically vaguely justified. Also it was established that the semantics used are mainly oriented on technical security experts and are not suitable for the audience targeted in this research, i.e. a wide range of experts with different backgrounds. In order to find a suitable basis for the semantics a research was made into the IAS literature and existing conceptual models of IAS. No model that would fit the purpose of this research in terms of the comprehensiveness, clarity, ease of comprehension and its conformance to the contemporary state of IAS was found among the conceptual models examined.

Therefore, this thesis (Chapter 3) introduced the Reference Model of Information Assurance & Security (RMIAS) which was developed based on the analysis of IAS literature and of the existing conceptual models of IAS (Chapter 2).

Returning back to the motivating scenario outlined in Section 1.2, the RMIAS was designed to tackle the second problem identified there, namely the absence of an agreed-upon understanding of the IAS domain and its main concepts among the members of a multi-disciplinary group involved in the discussion of security issues. The RMIAS provides a basis for the development of a commonly-agreed among the members of a multi-disciplinary group approach to IAS. The RMIAS facilitates the discussion of IAS issues by providing the set of key security concepts and interrelationships between them as well as by outlining drivers guiding security decisions. The RMIAS helps to identify and rectify the differences in understanding of IAS that experts with different backgrounds may have and which may hinder the effectiveness of communication about IAS.

Thus, Objective 1.B has been achieved and the RMIAS is the outcome.

Objective 2.B: *Evaluate the reference model of IAS, which underpins the semantics of the modelling technique, and to verify Hypothesis B (Section 1.4).*

The quality of the RMIAS was evaluated through a multiphase process in which several evaluation methods were used. The RMIAS was evaluated analytically by the model developer against the quality criteria of conceptual models suggested in [33]. Then, 26 experts were interviewed and their opinion regarding how the RMIAS satisfies the quality criteria were captured and analysed. The evaluation confirmed that the RMIAS reflects well the understanding of the IAS domain of the majority of the experts interviewed. In addition to this, the RMIAS was applied in a real life case study where it was used for the structuring of existing security policy documents and demonstrated its usefulness. The RMIAS was also evaluated in two workshops with MSc students where it was used for the development of a security policy document. The workshops along with the interviews confirmed that the RMIAS represents the IAS domain in a form and at a level suitable both for experienced and new to IAS users and that the RMIAS is complete and accurate at the chosen level of abstraction.

Hypothesis B, which is outlined in Section 1.4 and reiterated in Section 4.7, was corroborated by the evaluation conducted. Hence, it was confirmed that the RMIAS may be used as a basis for the semantics of a security-annotation technique.

Chapter 4 contains the description of the evaluation process and confirms that Objective 2.B has been achieved.

Objective 1.A: *Develop a modelling technique that allows the representation of IAS concerns in business process models.*

Based on the analysis of other security extensions, a security-annotation technique which is titled Secure*BPMN was developed and introduced in Chapter 6.

Secure*BPMN enables the members of a multidisciplinary group - experts with different backgrounds - who must be involved in the discussions of IAS to express their security-related knowledge in a clear, easily

accessible form. For that purpose, Secure*BPMN adopted the RMIAS as the basis for its semantics. Since Secure*BPMN was created for human comprehension and the promotion of communication about IAS, its syntax was designed to be cognitively effective, i.e. easily comprehended and remembered by users.

The main problem tackled by this thesis was formulated as follows (Section 1.2): *There is a need for an easy-to-learn and easy-to-use graphical IAS modelling notation, which will be accessible by technical and non-technical, security and non-security experts alike. The semantics of a notation must be built upon a shared understanding of the IAS domain amongst the experts involved in the security discussion and decision-making.* Secure*BPMN is a solution for this problem.

Thus, Objective 1.A, the major objective of this thesis, has been achieved and Secure*BPMN is the outcome.

Objective 2.A: *Evaluate the proposed IAS modelling technique - Secure*BPMN, and to verify Hypothesis A (Section 1.4).*

Secure*BPMN was evaluated both analytically and empirically. Well-established and widely used in the current literature evaluation frameworks were used in the evaluation process (Chapter 7). The analytical evaluation was carried out to test the cognitive effectiveness and ontological completeness of Secure*BPMN. The empirical evaluation experiment was designed based on the MEM [136] to test the usefulness, ease of use and an intention to use Secure*BPMN in future. The evaluation experiment was run with the groups of experts and MSc students. Notably, the experiment corroborated that both new to and experienced in IAS and BPMN users were able to use Secure*BPMN successfully after a one-hour training session. An extensive set of data received during the experiment also enabled drawing many more specific conclusions regarding the use and perception of Secure*BPMN by different groups of users as discussed in detail in Chapter 7.

Hypothesis A (Sections 1.4 and 7.5) was corroborated by the evaluation conducted. Thus, it may be concluded that Objective 2.A has been fully achieved.

8.2 Future Work

8.2.1 Future Work on the RMIAS

As mentioned in Sections 3.6 and 3.4, the RMIAS as with any other conceptual model of any domain requires a regular revision. In future, the author intends to maintain the compliance of the RMIAS with the rapidly changing landscape of the IAS domain.

Until now, the RMIAS was only applied to one case study. In the future, the RMIAS may be applied to organisations of various sizes, operating in different sectors. This will enable further improvement, refinement and, as anticipated, extension of the RMIAS. It is difficult to foresee at the moment all possible ways

in which the RMIAS may evolve. Currently, based on the continuous literature review and the feedback on the RMIAS, the following potential directions of refining the RMIAS may be outlined: (1) the extension of the categorisation of security countermeasures to included the categorisation by the time/reason of implementation (e.g. prevention, detection, recovery [61]); (2) the extension of the life cycle dimension with the deliverables expected from each stage; and (3) the extension of the information taxonomy.

During the development and evaluation of the RMIAS, the author was in contact with several representatives of Small- and Medium-size Enterprises (SMEs), who articulated a need for a security recommendation system for SMEs that would support IAS decision-making, would be easy to use, would not require a significant technical or security knowledge and that would help to identify security countermeasures for various scenarios. As pointed out in Section 4.4.2, the Agency which participated in a case study has also expressed an interest in a a security recommendation system. The RMIAS provides a suitable basis for the development of such system. The data base to underpin the recommendation system has already been developed by the author and the work on the system will be continued. The development of a standalone web-based security recommendation system based on the RMIAS will be carried out as an MSc project by a student in the group of Information Security& Privacy at the School of Computer Science & Informatics, Cardiff University. In the future, the system may be enriched with risk information derived from experts' judgement and from statistics based on historical data to enable the derivation of security recommendations using probabilistic risk assessment methods. The security recommendation system will pose many interesting questions for testing, particularly with regard to the trustworthiness and reliability of the recommendations produced. A range of experiments will be required to test the quality of the system as well as its acceptance by prospective end users.

The RMIAS provides a framework to enable users to think about and communicate about IAS. It helps to identify problematic areas and shows possible directions in a search for solutions. The RMIAS does not give precise instructions, a step by step guide for solving security issues or final answers. It rather prompts its users to ask right questions. In the future, the RMIAS may be enriched with a probabilistic risk assessment methodology which would provide instructions on how to classify documents, how to identify appropriate security goals for them and how to prioritise the goals. For this purpose, the RMIAS may be mapped with the existing risk assessment frameworks such as for example OCTAVE Allegro [118] or others.

In this thesis, the visual appearance of the RMIAS received some attention, but it was not a primary goal, rather the focus was on the completeness, accuracy and adequacy of the content of the model. Further research is required to improve the visual appearance of the RMIAS. The existing guidance on the cognitive effectiveness such as the TVND [30], or the Cognitive Dimensions of Notations (CDs) framework [192] may be used to refine the visualisation of the RMIAS. Alternatively, the cognitive effectiveness of the RMIAS may be heightened as a result of multiple interactions with IAS experts and individuals new to IAS. The question of how to develop a cognitively effective reference model is anything but trivial. The analysis and improvement of the visual appearance of the RMIAS may provide a basis for and stipulate the creation of a

guidance on the design of cognitively effective reference models, which as anticipated will be a version of an existing framework or theory tailored specifically for reference models.

The RMIAS is currently presented in a notation-free form which was found the most suitable form for the purpose of communicating the nature and complexity of IAS to a multidisciplinary group of experts - *"While the representation we select will have inevitable consequences for how we see and reason about the world, we can at least select it consciously and carefully, trying to find a pair of glasses appropriate for the task at hand"* [104]. In the future, it may be possible to formalise the RMIAS and present it, for example, as an ontology using the Web Ontology Language (OWL) [203] or in any other more formal way to enable the use of the RMIAS by computer systems. It is worth remembering though, as pointed out in [104], that while such transformation my be an interesting research exercise it is not what the RMIAS "*was intended to do*", but "*what it can be made to do*". It is further remarked in [104] that "*Yet with striking regularity, the original spirit of a representation is seen as an opponent to be overcome. With striking regularity the spirit gets forgotten, replaced by a far more mechanistic view that sees a data structure rather than a representation, computation rather than inference. Papers written in this mindset typically contain claims of how the author was able, through a creative, heroic, and often obscure act, to get a representation to do something we wouldn't ordinarily have thought capable of doing.*"

Security overlaps with other non-functional concerns such as reliability, safety and resilience. The methodology used in this thesis for the development of the RMIAS may be followed to produce reference models of reliability, safety and resilience. The analysis of the reference models of various non-functional concerns will allow to establish the differences and overlaps between them. The ways of integrating the RMIAS with conceptual reference models addressing other non-functional concerns may be investigated in order to create a comprehensive view of all (or at least several) non-functional requirements in an IS.

In this thesis, the RMIAS was exploited to stipulate the semantics of a security modelling extension for BPMN. In the future, the RMIAS may be used to underpin the semantics for security extensions for other modelling languages. The extensions based on the RMIAS may be developed for other business process modelling languages such as UML Activity Diagram and IDEF; for other behaviour modelling languages (e.g. use case diagram); for structure diagrams (e.g. class and component diagrams); for goal- and agent-oriented methodologies (e.g. Tropos [204]).

What could also be of interest for the research community is to develop a truly comprehensive model of IAS that would address all known IAS concepts relevant at all levels of abstraction and from various perspectives. To the best of the author's knowledge, although some attempts to develop an integrated IAS ontology exist [79], none of the research attempts have achieved a wide level of adoption by research or industry. The author is not aware of any research related to the development of a comprehensive multi-perspective conceptual model of the IAS domain.

8.2.2 Future Work on Secure*BPMN

Business process models are used during the requirements engineering stage of the IS life cycle. Hence, Secure*BPMN only helps to deal with security issues at the stage of security requirements engineering and only provides a view of security issues in business process models. However, IAS must be addressed consistently throughout different types of system models (i.e. structure, architectural, data models and other types of behavioural models apart from business process models) used during the security requirements engineering and design stages as well as throughout all stages of IS security development life cycle.

Therefore, in the future Secure*BPMN must be integrated with security modelling techniques which address security in other types of system models used at the security requirements engineering and security design stages. The consistent representation of IAS issues in a range of system models, and a smooth translation of security-annotations from a model of one type into a model of another type will lead to a better understanding of security issues at different levels of system design. It will ensure that security-annotations rendered at the business process modelling level are not lost, but are accounted for in the models developed at the later stages and are ultimately implemented. In future, a set of transformation rules must be defined to enable the translation of security-annotations rendered using Secure*BPMN into security-annotations of system models of other types.

There is already a proposal to extend Multi-Perspective Enterprise Modelling (MEMO) [205] for security modelling. The requirements for such an extension are outlined in [22], while the extension itself, to the best of the author's knowledge, has not yet been presented. Secure*BPMN provides a thoroughly elaborated security modelling technique to deal with security at the business aspect from the organisational perspective in MEMO and it may be incorporated into a security extension for MEMO.

The execution of security-annotations proposed was out of the scope of this thesis. At the moment, Secure*BPMN is an informal approach [176], i.e. it provides graphical notations with no further parameter specification. However, in the future Secure*BPMN may be extended to the level of a semi-formal approach by adding clearly defined attributes to accompany its graphical symbols [176]. Furthermore, the translation of graphical security-annotations rendered using Secure*BPMN into executable security configurations may also be investigated.

Secure*BPMN was designed as a generic security-annotation technique to suit a wide range of organisations. In future studies, the application of Secure*BPMN in the context of different organisations may be examined and sector-specific versions of Secure*BPMN may be developed. Currently, the author is working on a research project addressing this topic.

Ideally, a graphical syntax must be developed with multiple interactions with end users [13]. In this thesis, the syntax of Secure*BPMN was developed following the principles of the TVND [30] and there was only one interaction with prospective users regarding it, when users were requested to evaluate the cognitive effectiveness of the syntax during the evaluation workshops in a post-task survey. In the future, more

experiments may be set up to test the cognitive effectiveness of each symbol separately. For example, participants may be offered a choice of symbols to represent the same security concept and asked to choose which symbol better reflects the meaning of the concept. Similar experiments are described in [177].

During the evaluation of Secure*BPMN, it was only tested how well users security-annotate BPMN diagrams using Secure*BPMN and how well they interpret annotated diagrams since it was sufficient to answer the research questions posed in Section 7.3.3. The evaluation results received in this thesis may be investigated and analysed further to extract more information about how well groups interpreted different symbols or used them in annotation. This analysis will help to improve future Secure*BPMN training sessions. There is also a wide range of other experiments that may be conducted to provide additional information about the possible improvements of Secure*BPMN, and its advantages and limitations. It may be tested, for example, how well Secure*BPMN helps with the identification of possible security countermeasures in comparison with other security modelling techniques (similar experiments are presented in [201, 202]). The quality and quantity of security-annotations rather than their correctness and compliance with the grammar rules may be tested in future studies. The evaluation of Secure*BPMN sets up a basis for the comparative experiments and analysis. As soon as other security-annotation techniques are evaluated using the evaluation methodology suggested in this thesis, the comparative analysis between Secure*BPMN and other security-annotation techniques may be carried out.

As it was pointed out by one of the participants of the Secure*BPMN evaluation workshops, the acceptance of Secure*BPMN in practice is complicated by the fact that it is not a standardised method. In the future, Secure*BPMN will be brought to the attention of the working group of the OMG, an organisation who maintains BPMN. Secure*BPMN may serve as a stepping stone on the way to standardising an approach to the security-annotation of business process models expressed in BPMN.

8.3 Originality and Significance of the Research

This section revisits Section 1.7, where the contribution of this thesis is explained, and discusses the place of the research presented in the general body of knowledge and relates the results presented to other research.

The uniqueness of this research project is in the breadth and depth of the investigation carried out. In this project, two research topics were addressed in great detail - the representation of IAS knowledge and the development of a graphical security-annotation technique for BPMN. As discussed in Section 5.4.3.1, other security extensions for BPMN examined built their semantics upon the models of IAS developed elsewhere. In this PhD thesis, the author did not adopt a basis for the semantics of the security-annotation technique proposed from elsewhere as for example in [24, 96, 152, 183, 185], but after a careful investigation of alternatives developed its own model of the IAS domain, which was then evaluated to prove its merit and only after that was used to underpin the semantics of a modelling technique.

There are two main contributions of this PhD research project to science where a new knowledge was created as a result of the original research presented:

- **The Reference Model of Information Assurance & Security (RMIAS)**, and
- **Secure*BPMN, a novel graphical security-annotation extension for BPMN**.

The additional contribution of this thesis to science includes:

- *Review of the state of art in conceptual modelling of the IAS domain*,
- *Review of the state of art in extending BPMN for security modelling*,
- *Development and implementation of a multiphase procedure for the evaluation of a reference model of IAS*, and
- *Development and implementation of a multiphase procedure for the evaluation of a security extension for BPMN*,

The novelty and significance of the RMIAS and Secure*BPMN are discussed below. This then followed by the discussion of additional contribution.

8.3.1 The RMIAS

The RMIAS summarises the knowledge acquired by the IAS community of academics and practitioners to date in one all-encompassing model. It presents the key concepts of IAS and the interrelationships between them at a high level of abstraction in a form suitable for a wide range of experts with different backgrounds. The RMIAS approaches IAS holistically as a complex managerial issue. It does not limit the scope of

IAS to the technical aspect of security. The RMIAS aids in building an agreed-upon understating of the IAS domain, which a multidisciplinary team of experts requires before the experts may proceed with the discussion of security issues.

The key source that inspired the work on the RMIAS was McCumber's Cube [65], published in 1991, and its updated version - the model of Maconachy et al. [86] released in 2001 (Section 2.8.2.3). These models were included in security training and education programs in the US (Section 2.8.2.3). The RMIAS builds upon these two models and extends them with new security concepts to reflect the changing landscape of the IAS domain addressing a call for a regular revision of a conceptual model of the IAS domain expressed in [66, 61]. The RMIAS extends McCumber's Cube and the Machonachy et al. model in several ways: (1) it adds the legal security countermeasures and extended the scope of organisational and human-oriented countermeasures, (2) it enriches the list of possible information states with two missing states, namely creation and destruction, (3) it enriches the model with the information about the interrelationships about the concepts of the IAS domain, and about the drivers that stipulate security decision-making. It was pointed out previously by recognised security experts that the CIA-triad does not adequately reflect the contemporary state of IAS and requires an extension [66, 28]. Notably, the RMIAS addresses this call and extends the CIA-triad drawing upon the existing literature and other models analysed. The IAS-octave offered as an extension of the CIA-triad was evaluated by the experts of the IAS domain who confirmed its adequacy and completeness.

The true novelty of the RMIAS is in bringing together the segregated, discrete knowledge of the IAS domain in the form suitable for a wide range of experts with different technical, non-technical, security and non-security backgrounds. For example, in [87] the model distinguishes four types of security countermeasures, in [89] the model highlights the importance of ethics and culture, but they both overlook such a key concept as security goals. The RMIAS attempted to integrate the existing models of IAS with the knowledge of IAS captured in security standards and other literature and present it in one model. The merit of the RMIAS is the novel interpretation and representation of the existing IAS knowledge using an original research method.

There was only one other model [82] among the models analysed where the development process was documented and presented to the reader. The RMIAS development methodology is documented, including the inclusion/exclusion criteria, and, therefore, transparent and open to analysis.

The RMIAS was developed without the limitation to the context of business process modelling. Therefore, as it was confirmed during the evaluation process, the RMIAS may be used for a wide range of purposes such as education, benchmarking, consultancy, the facilitation of communication, security policy development and others.

The results of this part of the PhD research project are of interest to the world-wide community of IAS researchers and practitioners. The beneficiaries of the RMIAS are enumerated below:

- Research groups dealing with the capturing, representation and formalisation of IAS knowledge;

- Research groups interested in the evaluation of conceptual, reference models;
- Individuals novice to the IAS domain (e.g. students, experts in domains other than security) who require to understand the nature, complexity and diversity of the IAS domain;
- Security practitioners dealing with the development of security policies and security programs for their organisations; and
- Business owners who need to establish the IAS posture of their companies.

The interest in the RMIAS expressed so far, as discussed in Section 4.7, confirms the recognition of the value of the RMIAS by both academia and industry.

8.3.2 Secure*BPMN

Secure*BPMN was designed for the security-annotation of business process models expressed in BPMN to suit the needs of a multidisciplinary team of experts involved in the discussion of IAS and IAS decision-making. Secure*BPMN adopts an holistic approach to IAS from the RMIAS and enables the consistent representation of security countermeasures of different nature in BPMN models.

Secure*BPMN was originally inspired by the extension proposed in 2007 by Rodríguez et al. [24], a highly cited reference in the domain. The semantics of Secure*BPMN is more comprehensive than the semantics suggested in [24] and allows one to model a wide range of security concepts in addition to security goals/requirements addressed in [24]. Even in comparison with the recently proposed extension [152] (2014), the semantics of Secure*BPMN has a higher level of ontological completeness (Tables 5.5 and 5.6). What differentiates Secure*BPMN is that it extracts the security concepts from an adopted conceptual model of the IAS domain and introduces them into a security-extended metamodel of BPMN consistently, without unjustified exclusions or omissions as discussed in Section 7.2.1.

The syntax of Secure*BPMN was strongly influenced by the TVND [30], which was published in 2009, just a year before this research project has started. In the recent years, the importance of the cognitive effectiveness of the syntax of a modelling notation has received a lot of attention of researchers. The importance of cognitive effectiveness of security annotations in business process models has also been recognised [38, 177, 178]. This thesis is the first attempt to devote substantial effort to developing a cognitively effective syntax and to follow the scientific principles of the TVND consciously and consistently. Among all security extensions for BPMN analysed, the syntax of Secure*BPMN is the first to be evaluated in terms of its compliance with the principles of the TVND in such detail. This thesis brought the ideas of the TVND to the field of security-annotation techniques for BPMN.

In 2009, the detailed survey of nine attempts to integrate security and risk aspects into business process management was presented [175]. This survey identified several gaps in the research and Secure*BPMN

addressed the following two of them: (1) the need to extend a list of security goals - Secure*BPMN adopts the IAS-octave from the RMIAS which provides a justified and evaluated alternative to the CIA-triad; and (2) the need to improve business process modelling notations for security modelling - Secure*BPMN integrates security concepts in a de-facto industry business process modelling language and the first international standard in this area, BPMN.

In 2010, the representation of security in business process models was examined and summarised [176]. Two challenges facing research on security in business process models were outlined: (1) the development of a semantics covering all key security concepts and (2) the representation of this comprehensive semantics in "*an expressive yet intuitive manner*" [176]. Secure*BPMN built its semantics upon the RMIAS which offers a set of key security concepts and represents them in a cognitively expressive, easy-to-learn and easy-to-use manner as proved by the analytical and empirical evaluation.

In 2013, the syntax of six BPMN security extensions was analysed [177]. This analysis proposed two recommendations for the design of the syntax of security notations: (1) the use of scientific principles and (2) the involvement of users. It was also recommended to provide training on security to individuals involved in experiments. In this thesis, all three recommendations offered in [177] were addressed.

In 2014, a detailed analysis of 275 papers, published between 1993 and 2012 and related to security in Process-Aware Information Systems (PAIS), was conducted and presented in [178]. The security in PAIS was confirmed to be an interdisciplinary field of research which requires the knowledge of a broad range of disciplines. In view of this, the ability of Secure*BPMN to allow a broad range of experts with different backgrounds to express the security-related information they have in an intuitively clear manner appears relevant and useful to the domain.

The development and standardisation of security terminology and of the approach to security in PAIS was also designated as a research challenge in the field [178]. The RMIAS introduced in this thesis provides a basis for an agreed-upon approach to security and helps to agree upon the terminology. Another challenge mentioned in [178] was to extend beyond the technical orientation of the approach to security in PAIS and move towards the human-orientation which this thesis attempted to do both by incorporating a separate category of human-oriented countermeasures in the RMIAS and adopting it in Secure*BPMN, and by designing the syntax of Secure*BPMN specifically for human comprehension. A need for an holistic approach to security was also articulated [178], supporting the argument of this thesis and justifying the relevance and importance of the solution proposed in this thesis. As explained throughout this thesis an holistic approach to IAS determine both the RMIAS and Secure*BPMN.

The novelty of Secure*BPMN lies in its comprehensive semantics based on the RMIAS and in its cognitively effective syntax which was developed guided by the TVND [30].

This part of the research project helps to advance the fundamental knowledge about the development and evaluation of a graphical security-annotation techniques. The beneficiaries of this part of the research project

are enumerated below:

- Research groups interested in the development of domain-specific graphical modelling languages;
- Research groups dealing with security extensions for business process modelling languages;
- Research groups specialising in the development of cognitively effective syntax for modelling languages;
- Research groups dealing with the evaluation of modelling languages; and
- Business process modellers, security and business experts who require to represent their security concerns in a form which is easy to comprehend and communicate in business process models.

8.3.3 Additional Contribution

A strong emphasis was made in the research project on the evaluation of the solution proposed. As confirmed by the literature analysis (Chapters 2 and 5), none other conceptual model of IAS or security-extension for BPMN examined were not accompanied by such exhaustive, multi-aspect evaluation as the RMIAS and Secure*BPMN presented in this thesis.

The evaluation of conceptual and reference models is a challenging task and is a research topic in its own right [33, 99, 103]. The original multiphase evaluations carried out in this thesis to verify the quality of the RMIAS and Secure*BPMN provide examples of evaluation routes that are thorough, well-justified, transparent, and based on well-established frameworks. The evaluation routes may arm other researchers. The evaluation routes pursued combine the evaluation methods of different types, thus addressing drawbacks of separate evaluation methods. The evaluation conducted rely strongly on the involvement of people other than the developer ensuring the objectiveness of the evaluation results.

Among the models analysed, only the RMIAS was evaluated via interviews, workshops and a case study, while other models typically presented as position papers and rely for validation upon the expertise of its developer(s). The empirical evaluation of a model was performed in [82], but that evaluation used data analysis and did not involve explicit evaluation by experts.

The evaluation of the RMIAS was not limited to the confirmation of the completeness and accuracy of the model. The RMIAS was evaluated regarding all quality criteria suggested in [33]. Additionally, it was demonstrated empirically that it may be used for the structuring and organisation of existing security policy documents as well as for the development of a new security policy document by users who are not highly experienced in IAS.

The evaluation of business process modelling languages is also a topic of research which receives the attention of academics [136, 157, 165]. The evaluation of security requirements derivation and security-annotation methods has also recently begun to be examined by research community [177, 201, 202, 264,

263]. For Secure*BPMN, the evaluation addressed the quality of the semantics and syntax, and tested the effectiveness of the notation in practice. The evaluation was not limited either to analytical or empirical, but both types of evaluation were used to complement each other.

This thesis is the first attempt to evaluate a security-annotation techniques for BPMN using the MEM [136], which has been intensively used over the last several years for the evaluation of security modelling methods [201, 202, 263]

The contribution of this research project is also in the development and refinement of the evaluation exercises and all supporting martial including (1) the case study of Translate, (2) the security policy development exercise for MSc students, (3) the questionnaire for experts for the evaluation of a reference model based on the set of criteria adopted from [33], (4) the annotation and interpretation tasks, and (5) the post-task survey for the evaluation of the effectiveness of a security-annotation technique. Even the format of a journal paper does not allow researchers to provide a full description of the experimental material, not mentioning a conference paper which gives researchers a very limited space only to present their major findings. This thesis presents all evaluation material and describes the set up of all evaluation activities at the level of detail enabling other researchers to repeat the evaluation process with other models and modelling techniques.

Another valuable contribution of this thesis is a systematic acquisition and analysis of a substantial body of knowledge at the forefront of two research areas, namely the conceptual modelling of the IAS domain and the security extension of business process modelling languages. The analysis of conceptual models of IAS is presented in Chapter 2 and the analysis of security extensions for BPMN is presented in Chapter 5. While other reviews of security extensions for BPMN exist (e.g. [177, 179]), none of them present a literature review methodology used for the identification of extensions for analysis, or review such a large number of extensions in such depth as it is done in this thesis. In this thesis, every extension was examined with regard to a wide range of criteria including purpose, target audience, basis for the semantics, guidance for syntax, domain being modelled, evaluation method and others.

In this thesis, the systematic literature review methodology used for the identification of conceptual models of IAS for analysis is presented to guarantee the coverage and scope of the analysis. The conceptual models were examined in terms of the following criteria: purpose, contribution, basis for development/sources examined, visual representation and evaluation method. The author is not aware of other more detailed, systematic overviews of the conceptual models of the IAS domain.

8.3.4 Research Dissemination

Several aspects of this research have already been presented at three international conferences with the papers in conference proceedings being published (Section 1.8). In addition to this, two book chapters in a peer-reviewed book have emerged as the outcome of this research project (Section 1.8). At the moment, the author is working on a journal paper summarising the main achievements of the project.

The international conference presentations along with the number of presentations and workshops the author delivered in the UK to various academic and industry groups (Sections 1.8, and Tables 4.1 and 7.5) provided many opportunities for the research to be disseminated. The feedback and numerous comments received helped to consolidate both the RMIAS and Secure*BPMN.

Appendices

A.1 Members of a Multi-disciplinary Team involved in the IAS discussions

Business Expert - has the knowledge about business needs, business processes, collaboration and information sharing agreements, and information sensitivity. A Business Expert develops an enterprise IAS strategy. The main focus of a Business Expert is the profitability and competitiveness of the business, and overall business security.

IAS Expert/Officer - has the knowledge about enterprise security architecture. S/he serves as a bridge between the senior management and personnel of an enterprise. The Expert designs an enterprise security architecture, takes decisions about cost-security trade-offs; is involved in the development and implementation of the IAS strategy. S/he realises the overarching control over all IAS-related activities, including technical, organisational, human-oriented and legal ones. The Expert conducts the final check of a security-annotated model to ensure its completeness and compliance.

Another Domain Expert - has the detailed knowledge about a particular domain. S/he is responsible for the design and the subsequent implementation of domain-specific security countermeasures. The range of Domain Experts involved in the IAS discussions and the annotation of business processes depends on the organisational culture and is organisation- and industry-specific. The domain experts, who may be involved are listed below:

1) Computer and Network Expert - has the knowledge about enterprise computer and network architecture; is responsible for the implementation of the technical part of an IAS strategy;

2) Legal Expert - has the knowledge about general and industry-specific IAS- and privacy-related legislation, legal requirements and agreements in terms of information sharing and non-disclosure. S/he is involved in the modelling of legal security countermeasures and is responsible for the legal support of the IAS strategy;

3) Human Resources Expert - has the knowledge about personnel's IAS awareness and training needs, and is involved in the modelling of the human-oriented security countermeasures (e.g. training and motivation programs).

A.2 Structure of a modelling notation

Visual (graphical) notations are ubiquitously used in the domain of Information Systems throughout all stage of the ISDL for visualising, specifying and constructing systems, and for the enhancement of communication between system designers, software engineers, end-users and customers.

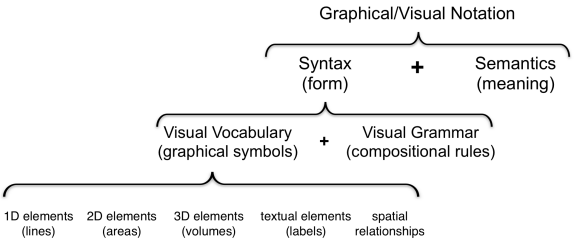


Figure 1: The structure of a visual notation [30]

The structure of a graphical/visual notation (as described in [30]) is depicted in Figure 1. A visual notation consists of semantics and syntax. Semantics, which is usually represented via a metamodel, defines the essential constructs of the notation and their meaning. Syntax, which is combined of Visual Vocabulary (graphical symbols) and Visual Grammar (compositional rules), defines the form for the representation of semantic constructs. Graphical symbols include lines, areas, volumes, labels and spatial relationships. Semantic constructs are depicted by graphical symbols.

A.3 Knowledge Representation

Levels of knowledge representation

Knowledge representation is described by its five roles [104]:

1. It is a surrogate which replaced the original object for research purposes;
2. It is a set of ontological commitments, which outlines the perspective and terms in which an object is considered;
3. It is a fragmentary theory of intelligent reasoning;
4. It is a medium of computation; and
5. It is a medium of human expression and communication.

A surrogate could never representation an object absolutely accurately - "*the only completely accurate representation of an object is the object itself*" [104]. However, an abstract representation of an original object or phenomenon is often required because it helps humans to deal with complexity.

The history of knowledge representation may be traced back to Socrates and Aristotle (and probably even earlier). Since then knowledge was represented for ideas sharing and communication. The advance of computers has invoked another role of knowledge representation which is to interpret human knowledge in a formal computer-accessible form.

Five levels of knowledge representation are distinguished in the knowledge representation science according to their computer-awareness [221]:

- Linguistic: the more computers distant level, it deals with arbitrary concepts, words and expressions of natural languages;
- Conceptual: the level which is nearer to the humans internal world models which operate with conceptual relations, primitive objects and actions;
- Epistemological: the level for defining concept types with subtypes, inheritance, and structuring relations;
- Logical: the level of symbolic logic which deals with propositions, predicates and logical operators;
- Implementational: the mostly computer-aware level which includes data structures such as pointers, lists etc.

The former three are the human-oriented while the latter three are the computer-oriented forms of knowledge representation. There is not strict division between the levels. The same representation may possess the characteristics of several adjacent levels [221].

Representing the IAS knowledge

Many researchers and practitioner argue the importance of formalising the IAS domain knowledge [222]. The formalisation of the IAS knowledge is not an easy or fast process, but it takes time and effort of many to be established. The scientific foundation in the security domain follows, rather than precedes practice as it also often happens in other domains. The foundation basis in the security domain is, in many cases, a synthesis of successful practices of various organisations and systems [222].

Different ways have been exploited to represent the knowledge of IAS. One is the development of the rigorous definitions of terms (e.g. [7, 223]). Glossaries and vocabularies are produced by standardising organisations (e.g. NIST Information Assurance Glossary [56] and ISO/IEC 27000 Vocabulary [55]) with an attempt to fix the meaning of security terms. This form of the IAS knowledge representation operates at the linguistic level and follows the Socrates and Aristotle scientific approach which is summarised in a famous Socrates saying: "*The beginning of wisdom is the definition of terms*."

The IAS domain knowledge may also be represented in the form of a concept and relationships diagram (e.g. [67, 59]). This form of representation uses such representation technologies as Entity-Relationship (ER) and UML class diagrams.

Another way to represent IAS knowledge is in the form of taxonomies and ontologies (e.g. [224, 225, 68]). The detailed examination of the existing security ontologies is presented in [79]. The ontologies typically represent IAS knowledge at the implementational level. They are computer-aware and intended for the automatic processing.

Another way to represent the IAS knowledge is in the form of a conceptual/reference model. The examples of conceptual models are considered in Chapter 2. This form of knowledge representation operates at the conceptual level. Conceptual models convey the knowledge of IAS in a human-intelligible way.

A.4 Overview of ISDLC and Security Development Life Cycle models

Table 1: The overview of the Information System Development Life Cycle (ISDLC) models.

InfoSec Handbook [105]	ISO/IEC TR 24748-1:2010(E) [226]		ISO/IEC TR 13335 [227]	NIST IR 7298 2011 [228]
Initiation	Concept	Concept	Planning	Initiation
Development/ Acquisition	Development	Development	Designing	Development
Implementation	Production		Implementing	
Operations/ Maintenance	Utilization	Operations/ Maintenance	Testing, acquisition operations	Operation
	Support			
Disposal	Retirement	Retirement	N/A	Termination

Table 2: The overview of Security Development Life Cycle models

InfoSec Handbook. SDLC [95]		The Microsoft SDL [218]	InfoSec Life Cycle [214]	SABSA Life Cycle [215]	Security Architecture Life Cycle [216]	Information System Security Risk Management Process [217]
N/A		Training	N/A	N/A	N/A	N/A
Initiation	Needs Determination	Requirements	Assess the current state of risk evaluating the existing security methods, measures and policies	Strategy & Planning	Architecture Risk Assessment	Context and assets identification
	Security Categorization					Security objectives to reach
	Preliminary Risk Assessment					
Development/ Acquisition	Requirements Analysis/ Development	Design	Based on the assessment, design a security posture by creating policies that effectively manage the risk to the system/network	Design	Security Architecture and Design	Risk analysis/assessment
	Risk Assessment					
	Cost Considerations and Reporting					Security requirements definition
	Security Planning					
	Security Control Development					
	Developmental Security Test and Evaluation					Controls Selection
	Other Planning Components					
Implementation	Security Test and Evaluation	Implementation, Verification, Release	Identify and implement the technical tools and physical controls necessary to manage risk	Implement	Implementation	Controls implementation
	Inspection and Acceptance					
	System Integration/ Installation					
	Security Certification					
	Security Accreditation					
Operations/ Maintenance	Configuration Management and Control	Response	Provide awareness training to the company to protect sensitive information through the cooperation and involvement of the employees.	Manage & Measure	Operations and Monitoring	N/A
	Continuous Monitoring		Audit the system/network to confirm that the controls and employees adhere to policy.			
Disposal	Information Preservation	N/A	N/A	N/A	N/A	N/A
	Media Sanitization					
	Hardware and Software Disposal					

Mapping with the stages of the security life cycle destinquished in the RMIAS:

- Security requirements engineering
- Security countermeasures implementation
- Security design
- Security management and monitoring
- Secure retirement of an IS

A.5 Translate. Case study

Business profile

Translate[1] is a small 15-person translation business established in 1993 by Mr White and Mr & Mrs Jones. Translate offers a wide range of translation services to large and small businesses, and individuals:

- Interpreters for conferences, Skype conference calls, presentations, negotiations and business meetings;
- Legal translations: contracts, agreements, expert opinions;
- Technical translations: product descriptions, user guides, manuals, handbooks.

By the nature of its business the staff of Translate has access to sensitive information of its customers. Translate staff often works directly at business customers' offices. Business customers are concerned about confidentiality of their information. Individual customers are concerned about the confidentiality of their private information.

Written documents for translation may be submitted to Translate by post, fax, email or via a company web-site. Translate could send the documents back to a client by any pre-negotiated way. When sending a translated document back to a customer Translate marks a document as "Proprietary" (according to its classification scheme). The Office Administrator in Translate sorts the post every morning at 10 am. Envelopes marked "Confidential" are forwarded unopened to a recipient. If a recipient is not specified then the Administrator opens the envelope in order to identify the recipient.

Translate has a web-site for promoting its services. Customers may upload their documents via the web-site. The web-site is hosted externally. Documents submitted for translation via the web-site are saved in a special folder on the external server. Mrs Jones accesses the document via ftp using FileZilla at 10 am every weekday, uploads them on to the Translate server and then allocates the work to translators (by email).

All drafts and working versions of translated documents are stored on the local machines. Original documents submitted for the translation, completed and archived translated documents are stored on the File & Print Server (usually within 18 months, unless other requirements are specified by a customer). Financial information is stored partially on the server and partially on Mrs Jones' laptop.

There are nine desktop computers in the office. All machines in the office are connected into a LAN (Local Area Network). All translators and business owners use the company laptops, which could also be connected

[1]The case study is based on the real company located in Australia. The name of the company was changed, missing details were added based on other case studies. Before administering the case study to the participants, the case study was validated with three academics specialising in Information System Design and IAS. The Translate case study is a generic case study of an SME with prolate security problems.

to the LAN. All files are stored on a File & Print Server located in the same room. All printers are connected to the Server. A central modem is integrated into the router, providing the Internet access to each machine on the LAN. A firewall keeps unwanted public traffic from accessing the LAN.

Translate uses MS Office: for translated document (Word), email and correspondence (Outlook), customers and orders databases (Access); HR records (Word, Excel). They use Sage for financial accounting. Internal and external communications are done via Skype, mobile phones or landline.

Problems

In 2011-2012, Translate had experienced some difficulties that undermined its effectiveness and shattered customers' trust.

In March 2011, the marketing officer sent an advertising email to all existing business customers. The text of the email included information about several existing customers and projects Translate worked on for them. Three out of the mentioned in the email customers approached Translate with a complaint: they believed that confidential information was revealed.

Mrs Jones (the owner), a mother-of-three, has a very active social live. She works from 10.00-14.00 in the office. She also works 1-2 hours from home in the evening. Mrs Jones usually works at home and in the office from her laptop. Occasionally, Mrs Jones uploads data on a USB stick to take some work home or she takes paper documents. On the 15th January 2012, she spilt a cup of tea over her laptop (a cold cup, actually). On that day she was working on the invoices, all information was lost and she had to spend the next day redoing the work.

In May 2012, Mr Jones discovered that two members of staff were making negative remarks about Translate's customers on Facebook. On several occasions, a customer reported that a translated document was not received by email in due time. The office administrator confirmed that a document was emailed on a specified day. It was not finally established whether the administrator emailed a document to a wrong email, or a customer deleted email as a spam.

The major problem, which, in fact, urged on all forthcoming changes in Translate, was a conflict with the IT manager. It was discovered that the IT manager used his admin password to access the company's confidential financial information and personal information of the staff. The IT manager was dismissed in September 2012. After the IT manager had left, it was revealed that he destroyed a list of potential customers the communications officer was working on. It was also suspected that the ex-IT manager took with him a list of all existing customers.

Recent Changes

After the aforementioned problems Translate undertook some major changes to its business operations. In October 2012, Translate outsourced the IT services to IT4U - a well-established IT service provider. IT4U looks after all the office equipment of Translate. The IT4U staff visits Translate's office twice a month, on other occasions the support is provided by phone, email or via Skype. IT4U also supports the website of Translate. IT4U was well equipped to help Translate find the right cloud solution. Since November 2012 all original and translated documents, as well as financial documents and contracts are stored on the cloud. Every member of staff has a username and password that allows him/her to access, change or delete documents. IT4U handles all IT-related contracts and billing for Translate. The managed cloud service means that Translate can create/delete accounts for its employees with a simple call or email to IT4U.

In December, Translate hired two new translators specialising in Asian Languages (permanent contracts). Translate plans to hire several freelance translators for a short (2-3 months) period of time during 2013-2014 to assist with a large forthcoming project.

Translate information classification scheme is presented in Table 3.

Your Challenge

Your group is asked to assist the business owners in developing a comprehensive Information Security Policy Document (ISPD) for Translate. Mr White and Mr Jones recently came across a Reference Model of Information Assurance & Security (RMIAS). They believe that the model could help to structure the existing security policy document and to identify omissions in it. The policy should reflect the needs of the Translate staff and customers. The policy should be implementable, easy to understand and must balance protection with productivity. The policy should be as complete as possible and cover all major activities of Translate.

Additional notes: If any required detail is not available, you are to make an assumption. Ensure that you note the assumptions made. Try to keep the number of additional details to a minimum.

Table 3: Information Classification Scheme of Translate

Label	Description	Examples
Public	Information could be made public without any implications for Translate. Translate is concerned about completeness and accuracy of information. Access: no restrictions	Brochures, Press-releases, Video-releases deployed on Youtube.com, information about Translate available on the Internet - on the company's web-site, in various social and professional networks etc.
Proprietary	Unauthorised accesses to this information may lead to critical consequences. Access: staff of Translate	All original customers' documents, translated documents in paper or electronic form; Information about events, meetings, and negotiations outcomes
Restricted Sharing	Protection of information from external access is crucial. Unauthorised access to this data could influence the business effectiveness, cause a financial loss, or shatter customers' trust. Access: staff of Translate	Customers' data, internal meeting protocols, telephone books, personnel data, accounting data, passwords, information on security weaknesses, a list of prospective customers, contracts, financial statements.
Confidential	Protection of information from unauthorised external or internal access is critical. Access: Business owners only	Salaries, Bonuses, Expansion plans, Financial and Audit reports, some contracts

A.6 Security Goals in the RMIAS

A.6.0.0.1 Accountability Accountability is defined in the ISO/IEC 27000 family of standards as the "*responsibility of an entity for its actions or decisions*" [55]. According to ISO/IEC 13335-1, accountability is "*the property that ensures that the actions of an entity may be traced uniquely to the entity*". The National Information Assurance Glossary[2] [56], defines accountability as the "*principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information*".

These definitions reveal two facets of accountability:

- Technical facet, which refers to the ability of the ICT components of an IS to record and trace all actions with information. However, the fact that user's actions are recoded and traceable does not on its own imply that the user could be held accountable for his/her actions (more detailed example of this issue in a banking domain is outlined in Section 4.2.5).
- Non-technical facet, which refers to legal, ethical, cultural and organisational drivers that force a person or an organisation to be responsible for his/her/its actions.

Often, an IS is designed with the security requirement to hide confidential information from unauthorised users which is exclusively achieved via access control. The unconditional reliance on access control opens a new problem. The information, that is once revealed (either by mistake or deliberately), becomes uncontrolled - "*[i]t's like focusing all one's attention on closing the barn door and ignoring what might happen to the horses after they've escaped*" [120]. With information sharing as a day-to-day reality the security rule "hide it or lose it" is not always valid. Information intentionally escapes the organisation's safe boundaries. Hence, an IS must enable the proprietor of information to control it not only within its secure boundaries, but also outside them.

Accountability highlights the need for an IS to be able to control the appropriate use of information within and outside the perimeter of an organisation. Different types of security countermeasures may be exploited to ensure accountability. Technology, policies, education and law aid in holding internal and external misusers of information responsible for their actions.

Only people (or organisations) may be held accountable for their actions (Table 3.2).

[2]The National Information Assurance Glossary, which is published by the Committee on National Security Systems (CNSS), was created to resolve the differences between the definitions of terms used by the U.S. Department of Defense (DoD), Intelligence Community and National Institute of Standards and Technology Glossary (NIST).

A.6.0.0.2 Auditability (Transparency)

Along with hiding information from unauthorised users, IAS is also concerned with making an IS transparent and auditable for authorised users. This is declared in a wide range of documents: the American Institute of Certified Public Accountants standards, the Organisation for Economic Cooperation and Development (OECD) Principles of Corporate Governance [125], the King report on Corporate Governance in South Africa [124], the Turnbull Report [121, 123] in the UK and the Sarbanes-Oxley Act [115] in the USA.

Auditability refers to the ability of an IS to monitor all actions within the IS, performed either by machines or humans. The monitoring should be persistent with no possibility to overcome or turn it off [122, p.246]. Auditability may be considered as a fundamental security goal, which supports other goals. For example, neither accountability nor non-repudiation are possible without the auditability of a system.

Auditability is applicable to all six components of an IS (Table 3.1). It refers to the monitoring of data provenance and use, of human behaviour, of the correctness of business processes, and of the hardware, software and network performance.

With regard to the overlap between accountability and auditability, the following must be noted. The technical facet of accountability correlates with auditability. However, auditability is the monitoring of a system in a global sense, whereas accountability is limited to tracing actions to particular users. Moreover, accountability includes the legal connotation which is not captured by auditability. If a multidisciplinary team of experts considers various security goals that must be addressed and works with a set of goal which omits accountability, than it may cause problems. The logical leap from auditability to accountability is possible, but it is time-consuming and strongly depends on the experience and knowledge of experts involved in the discussion. The acknowledgement of accountability as a discrete security goal immediately brings to the attention of experts the category of threat that must be addressed, namely threats related to problems of holding misusers accountable even if the technical proof of misuse is present.

A.6.0.0.3 Authenticity & Trustworthiness

Although the meaning of authenticity seems to be quite intuitive, there is a range of varying interpretations of this term. The definitions of authenticity derived from different sources are outlined in Table 4. Two approaches to authenticity could be distinguished. First, authenticity as the genuineness, validity and conformance to reality of information itself [66]. Second, authenticity as the ability to verify entities providing information [55, 122, 49, 56].

Table 4: Definitions of Authenticity

Reference	Definition
ISO/IEC 27000 [55]	*Property that an entity is what it claims to be.*
CNSS [56]	*The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.*
Parker [66]	*Validity, conformance, and genuineness of information.*
Anderson [49]	*Authenticity means integrity plus freshness: you have established that you are speaking to a genuine principal, not a replay of previous message.*

In line with [55] and [56], Neumann [122] relates authenticity with the ability to verify users. Parker [66, p.226] criticises Neumann saying that "*[Neumann] prefers to reserve authenticity to apply to identity of system users rather than to information, to avoid confusion - even though he readily applies integrity to systems, data, and people.*"

According to Parker, authenticity reflects "*the conformance to reality*" and "*extrinsic value or meaning of the information with respect to external sources*". Parker states that even the information provided by an authorised user, whose identity is verified, does not necessarily comply with authenticity when a verified and authorised user misrepresents information, e.g a software distributor replaces the name of the publisher on a software product with the name of a more popular publisher [66]. Despite the fact that the information is complete and its integrity is not violated, the information does not confirm to reality.

The identity of a user may be established using modern technology. However, authenticity in Parker's interpretation does not depend on the identity of an information provider, but reflects the "absolute truthfulness" of information which is hard to establish. In practice, the Parker's approach to authenticity is hard to implement. It requires the assurance that information is compliant with the information which is received from other sources so that its conformance to reality is established.

In the context of the RMIAS and this thesis, authenticity is understood in line with the definition in [56] as the property of "*being able to be verified and trusted*." According to the adopted definition, authenticity also includes the notion of trust. Trust is an essential concept of the IAS domain and should be addressed in any model. The RMIAS embraces trust within authenticity. In order to make this more explicit, the name of this security goal is declared as *authenticity & trustworthiness*. This security goal is particularly important in information sharing communities because it covers the interactions of an IS with external parties.

A system should encompass the ability to verify an end-point device (where an end-point device may be either a machine, a network or a human-being providing input information for an IS) to establish trust in

it. Trustworthiness may be established based on (1) the verification of the user's identity (authenticity) and (2) the verification of acting on a free will (for human beings) and/or the correct functioning for technical devices and networks (integrity).

The problem with establishing trustworthiness of an end-point device is that it is pointless to trust a malicious end-point device claiming itself being secure. Currently, for the majority of ISs a genuine user is the one who knows/has verification attributes. If a thief has a stolen credit card and uses it to withdraw money from someone's account, as long as the thief knows the PIN, he/she is trusted since he/she has passed the verification process. As another example, a user is forced to withdraw money from his account under compulsion. To ensure trustworthiness of a user, in the example with the stolen credit card, a system should consider the trusted person not the one who has a card and knows the PIN, but only the owner of the credit card, who does not act under compulsion. In order to acknowledge the personal identity fingerprint scanning or iris recognition may be used. It is more challenging to check that a user is acting on free will. Physiological parameters such as pulse rate and heartbeat may be gauged to ensure this.

The trustworthiness of data depends not only on its authenticity (the sender's identity verification), but also on the trustworthiness of the networks through which it is transmitted. If information is passed from a verified device via a perilous connection, the information can no longer be trusted. Untrustworthy networks abolish trust in any end-point device.

Parker [126] claims that if a complete set of security goals to be created to cover all possible threats to information then threats caused by social-engineering attacks should also be taken into the consideration. The threats, which are related to social-engineering are getting more diverse and widespread. In the RMIAS, authenticity & trustworthiness address threats related to deception and social-engineering. The majority of social-engineering attacks are caused by poor verification or the lack of verification. Verifying and establishing trust in a device, requesting information, may prevent many social engineering attacks.

A.6.0.0.4 Availability Availability is defined by both ISO/IEC 27000 [55] and the National Information Assurance Glossary [56] as the property of being accessible and usable upon demand by an authorised user. A denial of service attack is an example of the breach of availability. Neumann [122, p.246] explains that a system must be protected against both accidental and malicious denials of service, and must be available for use whenever it is expected to be operational.

Parker [66] understands availability as the property of information, rather than a property of a system and defines it as the "*usability of information for purpose*". According to Parker [66], an example of the breach of availability is the intentional deletion of the file name from a file directory by a rejected programmer. In this case, an organisation still physically possesses the data in the file, but does not have it available. The severity of the breach of availability depends on whether it is possible to restore the data or the data is destroyed without any chance to restore it.

Parker also suggests utility as another security goal which he defines as the usefulness of information for specific purposes [66]. The breach of utility may happen when an employee accidentally erases an encryption key. The organisation still possesses the data, but usefulness of the data is lost. The severity of a utility breach correlates with the ability to restore the data to its useful state. The notion of utility is important, but considering it as a separate security goal is illegitimate since it is already included in the meaning of availability and integrity. It is not legitimate to claim that encrypted data is available, if the encryption key is lost. Following [55] and [56], the RMIAS approaches availability as the property of being accessible and usable when required by authorised users.

In the RMIAS, availability is applicable to all components of an IS. The meaning of the availability of data is discussed above. The availability of people refers to the fact that people are ready and capable of performing allocated actions whenever required. The availability of business processes means that business processes are described and implemented (and automated, where required). The availability of software, hardware and networks means that these system components are available and operational when they are required by authorised users.

A.6.0.0.5 Confidentiality Confidentiality is the cornerstone of the IAS domain. It is the security goal with the least controversy over its definition. ISO/IEC 27001:2005 [114] defines confidentiality as "*the property that information is not made available or disclosed to unauthorized individuals, entities, or processes*". Parker [66, p.223] defines confidentiality as the "*limited observation and disclosure of knowledge*". For example, if the PIN code of a bank account is eavesdropped by a thief while a customer is being served by an ATM, the thief has breached confidentiality of information. The PIN is still available to the customer, its authenticity and integrity are not affected.

Confidentiality refers to the breaches which happen as a result of an unauthorised user disclosing or observing sensitive information. Confidentiality deals with the "Who can/cannot access information?" question and comes down to the prevention of the disclosure of information by unauthorised users.

A.6.0.0.6 Integrity Integrity is another complex and debatable concept. ISO/IEC 27000 [55] defines integrity as "*[t]he property of protecting the accuracy and completeness of assets.*" The National Information Assurance Glossary [56] defines integrity as "*[t]he property whereby an entity has not been modified in an unauthorized manner.*" The glossary is concerned with the fact that information is edited only by authorised users, while the ISO/IEC 27000 concentrates on the state of data, characterised by completeness and accuracy.

McCumber [65, p.330] states that "*[t]he definition of integrity must include the broad scope of accuracy, relevance, and completeness.*" According to Neumann [122], "*[d]ata integrity relates to data items being as they should be*", "*system integrity relates to extent to which hardware and software have not been altered inappropriately*" and "*personnel integrity relates to individuals behaving in an appropriate manner*" [122,

p.2]. Integrity is defined by Parker as the "*completeness, wholeness, and readability of information and quality being unchanged from a previous state*" [66].

In the RMIAS, the integrity of information (data) covers both completeness and accuracy, and the absence of unauthorised (or unwanted) modifications. Following Neumann [122], integrity is applied to all other components of an IS as well as to information. The integrity of the ICT components of an IS (hardware, software and networks) refers to the absence of unauthorised alterations in them and to their ability to function as intended. The integrity of people relates to the appropriate behaviour of personnel acting according with security policies and following pre-defined business processes. The integrity of a business process refers to the sequence of activities it outlines being accurate, complete and lacking unauthorised modifications.

A.6.0.0.7 Non-repudiation Even after a personal conversation one of the parties involved in the conversation may later deny something that was said or done. The issue is exaggerated in an impersonal electronic communication. A bank client may deny the electronic withdrawal of funds from his account. The sender of a malicious email may deny the fact of sending.

Neumann [122, p.212] understands non-repudiation as a problem related to authentication and describes it as the assurance of genuineness. Anderson [49] defines non-repudiation as "*the ability for the principals in a transaction to prove afterwards what happened*". Anderson states that to achieve non-repudiation a system should provide a way for any participant to prove participation or non-participation [49, p.343].

Non-repudiation is defined in ISO/IEC 27000 [55] as the "*ability to prove the occurrence of a claimed event or action and its originating entities, in order to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event*". The National Information Assurance Glossary [56] defines non-repudiation as the "*[a]ssurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.*"

The definitions discussed above cover non-repudiation from the system engineering perspective. There is also a legal connotation of non-repudiation [127]. The controversy between engineering and legal aspects of non-repudiation lies in the following. From the systems engineering perspective the technical proof of an occurrence/non-occurrence of an event (e.g. log files) or the proof of binding a user to specific actions (e.g. digital signature) guarantees non-repudiation. However, such proof that an IS may provide is not always valid in the legal context [127]. In legal terms, such proof is challenged because it may be forged, be a result of dishonest actions or be received under duress.

In the context of the RMIAS, it is important to note the difference between the system engineering and legal meaning of non-repudiation and to avoid the substitution of the legal connotation with the system engineering one. In the RMIAS, non-repudiation refers not only to the ability of an IS to provide a technical proof of the occurrence of an event, but to provide a proof which is valid in a legal sense. This ability leads

to the minimisation of potential technical, legal or organisational problems related to the repudiation of any aspect of interactions between parties [14, p.461]. The notion of non-repudiation is particularly important in cross-organisational business processes.

A.6.0.0.8 Privacy

"There is no security without privacy."
B. Schneier [45, p.70].

A set of security goal would be incomplete without privacy. This section does not aim at providing a detailed discussion of the meaning of privacy from different perspectives, such discussion with the excursion into history may be found in [128]. This section outlines how privacy should be understood in the context of a secure IS design and how it is defined in the RMIAS.

Although some privacy-preserving principles are still not consistently enforced by law in some countries and legislation often struggles to keep abreast with the rapid evolution of ICT, the privacy-preserving legislation provides an extensive set of requirements for privacy in an IS [130]. The definition of privacy adopted in the RMIAS explicitly refers to the obeyance of privacy legislation.

In addition to pointing out at a need for obeying privacy legislation, the definition of privacy adopted in the RMIAS draws on the conception of privacy as "*a social arrangement that allows individuals to have some level of control over who is able to gain access to their physical selves and their personal information*" [132]. Every individual has different apprehension of privacy, for some personal data are more sensitive than for others. An IS should implement mechanisms allowing users to control their personal data according to their individual needs and enabling users to specify their privacy preferences regarding their private data stored in an IS. The approach to privacy which builds upon the involvement of individuals into the specification of their privacy requirements in an IS is adopted, for example, in e-government systems [133] and some social networks (e.g. Facebook [134]).

A.7 Security Countermeasures Types in the RMIAS

The lists of security countermeasures, which are outline in this appendix, are by no means exhaustive and are only intended to explain the nature of a security countermeasures type.

Technical Security Countermeasures

Technical security countermeasures refer to the technical means which are exploited to achieve security goals. For example, identification, authentication and authorisation are technical countermeasures which help to achieve integrity, confidentiality and accountability. Cryptography is one of the main technical countermeasures which protects both integrity and confidentiality. Other examples of technical security countermeasures are biometrics, digital signature, firewall, intrusion detection and prevention systems, anti-virus software, anti-spyware, anti-malware, penetration and vulnerability testing, log and traffic analysis, data leakage prevention systems, access control etc. One of the existing taxonomies of technical security countermeasures could be found in [225, 234].

Organisational Security Countermeasures

Organisational security countermeasures refer to the administrative activities which help to build and maintain the environment where selected security countermeasures may be effectively implemented, managed and monitored.

These are the examples of organisational countermeasures:

- Security strategy, which defines the security requirements in terms of purpose, goals, scope, resource allocation, authorities, responsibilities, and compliance;
- Security policy;
- Processes or procedures;
- Governance;
- Audit;
- Compliance with security practices and best standards;
- Business continuity and contingency planning;
- Physical security;
- Personnel management (e.g. employment and retaining suitable personnel for security roles);
- Clear security-related duties and obligations;

- Senior management involvement, etc.

Human-oriented Security Countermeasures

Human-oriented security countermeasures address the impact of the human-factor on IAS. Many authors argue that people play the most essential role in achieving security [135, 46]. According to the *Information Security Breaches Survey* [6], in 2014 employees caused security issues in 58% of large and 22% of small companies. The same survey states that as much as 31% of the worst security breaches were due to the human-factor.

The existence of security policies and technical tools does not necessarily imply that they are obeyed and used. An organisation should ensure (via education, training, motivation and other means) that security instructions are respected at the personal level. With cross-organisational information sharing, people who must be security-trained include not only employees of a particular organisation, but also its customers and employees of other organisations involved in information sharing who handle information of the organisation [54, Sec. 3.6-3.7].

Human-oriented countermeasures in many cases strive to overcome the mechanical following of security instructions. End-users should understand security countermeasures not only as organisational solutions, but as something that directly relates to their day-to-day activities. Without the full support of individuals dealing with information and without their clear understanding of the rational behind security countermeasures, the effectiveness of many technical, organisational and legal countermeasures will be hindered [235].

Human-oriented security countermeasures include, but are not limited to

- Education and training - people must have knowledge and skills to use new technology and follow security policies [236];
- Awareness about newly invoked threats (e.g. in the case of social-engineering attacks hardly any technical security countermeasure might help, while awareness might [135]);
- Ethics;
- Culture;
- Motivation - security awareness and education should be supported by motivation which may be based on reward or penalties [61].

Legal Security Countermeasures

Legal security countermeasures refer to the use of legislation and contractual agreements for information protection. With cross organisational information sharing, information often escapes the boundaries of an

organisation. In such cases neither technical nor organisational measures could help to protect information. In these situations, legal countermeasures are indispensable. Similar situation is encountered with the proliferation of social networks which leads to the exposure of sensitive personal information on the Internet on a great scale when no other than legal countermeasures might provide the adequate protection of private information.

These are only a few examples of legal countermeasures:

- Established information ownership [108];
- Legally agreed and enforced information classification and labelling schemes. The creator of information owns and classifies information. Legal agreements force other organisations to respect the owner's classification and handle information according to the owner's requirements;
- Service-level agreements. The agreements with service providers define the provision against denial of service, impose penalties for inappropriate information handling or accidental loss/leakage of information;
- Job contracts and employee non-disclosure agreements;
- Third party non-disclosure agreements which place responsibility on third parties for appropriate information handling of information and impose penalties for information misuse.
- Law (e.g. copyright law [237], the Data Protection Act 1998, etc.).

A.8 Types of Evaluation

A conceptual model as well as a modelling language may be evaluated analytically or empirically [27, 165]. While empirical evaluation involves prospective users of a model or modelling language, analytical evaluation does not. Analytical evaluation is conducted by an evaluator/researcher(s) usually with the exploitation of an evaluation framework and based on the examination of available information about the evaluated object. Both types of evaluation have their advantages and disadvantages.

One of the advantages of analytical evaluation is that it is usually performed by experienced individuals, who have extensive knowledge of a evaluated object and of an evaluation technique. Evaluators are well motivated and dedicated to evaluation and analysis. Analytical evaluation allows the consideration of an object in greater depth since it is less restricted in terms of time and cost than empirical evaluation. The time and cost of analytical evaluation is lower because it does not require a large number of people to be involved and motivated [13]. Analytical evaluation is often conducted by the model or modelling technique developers or by a small in number group of researchers. In research projects, a decision to give preference to an analytical evaluation is often dictated by time and budget restrictions. One of the drawbacks of analytical evaluation is that the results are influenced by the perspective and background of the evaluator(s). Also, if evaluation is performed by the developer of an evaluated model or modelling language, evaluation may be biased.

The merit of a method embedded into a conceptual model or of a modelling technique could only be realised if it is effective in practice. A method ("knowledge how") as opposed to a thesis ("knowledge that") is not either true or false, but is either effective or not [37]. Where analytical evaluation could only make predictions about the effectiveness of a method and its potential adoption in practice, an empirical evaluation may refute or corroborate results of analytical evaluation as well as predictions from theories such as for example the Theory for Visual Notation Design [31].

In addition to a higher cost and difficulties in administration, in comparison with analytical evaluation, empirical evaluation suffers from other drawbacks. A low motivation of participants and a danger of the misunderstanding of an evaluated model or method by participants are only some of them. Participants are also often affected by additional factors that may not always be accounted for by research (e.g. mood, language understanding, attitude to an experiment). Furthermore, several empirical studies with a significant number of participants should be conducted and the results should be repeated before any conclusion may be taken as final.

A.9 Security Policy Statements Collected During the Workshops

Table 5: Information Security Policy Statements developed during the workshops. Part 1 of 4.

N	1. Form	2. Sensitivity	3. Location	4. State	5. Security Goal	6. Security Countermeasure Type: Description
1	Electronic	Proprietary	Processing	Controlled	Privacy	Human-oriented: To ensure that all employees of Translate are timely educated regarding their access rights and consequences of private information misuse.
2	Electronic	Restricted Sharing and Confidential	Destruction	Controlled	Availability	Organisational: An employee must not delete information classified *Confidential* or *Restricted Sharing* without an approval of the management team.
3	Electronic	Restricted Sharing and Confidential	Destruction	Partially Controlled (Cloud)	Availability	Technical: An employee's account must not be granted right to delete a document classified *Confidential* or *Restricted Sharing*.
4	Electronic	Restricted Sharing and Confidential	Processing, Storage	Controlled	Availability	Technical: A back-up copy of all files marked *Confidential* or *Restricted Sharing* must be created each night. No employee to have rights to delete/change backup files.
5	Paper	Public	Creation	Controlled	Integrity	Organisational: Documents labelled *Public* may only be disseminated only after being reviewed by a manager (and a legal adviser, where needed).
6	Paper Electronic	Public	Creation	Controlled	Non-repudiation	Legal: A written consent of a customer must be received prior to using the name in an advertisement.
7	Paper	Proprietary	Processing	Controlled	Auditability	Organisational: Only the translator(s) working on a case may access original paper documents of the customer (need to know). Access to *Proprietary* documents must be signed for and Translate to retain access log book.
8	Paper	Proprietary	Storage	Controlled	Privacy	Organisational: Translate must not store copies of original customers documents after the receipt of the translated documents is confirmed by a customer.

Table 6: Information Security Policy Statements developed during the workshops. Part 2 of 4.

1	1. Form	2. Sensitivity	3. Location	4. State	5. Security Goal	6. Security Countermeasure Type: Description
9	Electronic	Restricted Sharing, Confidential	Transmission	Uncontrolled	Confidentiality	Technical: Documents marked as *Restricted Sharing* and *Confidential* may be sent by email only in an encrypted and/or password protected form.
10	Electronic	Restricted Sharing, Confidential	Transmission	Uncontrolled	Confidentiality	Organisational: A password must not be sent by the same method as a password protected document. A password may be exchanged using a phone, Skype, or may be pre-agreed between the employees of Translate
11	Electronic	Proprietary, Restricted Sharing, Confidential	Processing	Controlled, Partially Controlled	Auditability	Technical: Access to electronic documents classified *Proprietary*, *Restricted Sharing* and *Confidential* must be logged.
12	Verbal	Restricted Sharing	Transmission	Partially Controlled	Authenticity/ Trustworthiness	Human-oriented: No sensitive information to be conveyed over the phone/Skype/email to IT4U (IT service provider) or any other third party without an authorisation. An employee must not reveal its account password to any third party at any time.
13	Paper	Proprietary, Restricted Sharing, Confidential	Storage	Controlled	Confidentiality	Organisational: Visitors, including customers and the staff of IT4U and other service providers, must not be left unattended in any room where classified documents are kept.
14	Verbal	Proprietary, Restricted Sharing, Confidential	Processing	Controlled	Confidentiality	Legal: An employee to sign a confidentiality agreement as a part of the introductory activities.

Table 7: Information Security Policy Statements developed during the workshops. Part 3 of 4.

1	1. Form	2. Sensitivity	3. Location	4. State	5. Security Goal	6. Security Countermeasure Type: Description
15	Verbal	Proprietary, Restricted Sharing, Confidential	Transmission	Uncontrolled, Partially controlled	Confidentiality, Privacy	Organisational: A care should be taken to avoid eavesdropping while discussing job-related matters over phone/Skype in a public place (awareness of surroundings).
16	Electronic	Any	Processing, Storage, Transmission	Partially Controlled	Confidentiality	Legal: IT4U, a supporting IT company, must be made aware about Translate's security policies and document classification scheme. IT4U must be legally bound by a contract to obey security policies of Translate.
17	Electronic	Any	Processing	Controlled, Partially Controlled	Integrity, Availability	Organisational: As a part of the employment termination process, all access rights must be timely removed.
18	Electronic, Paper	Any	Processing	Controlled, Partially Controlled	Confidentiality, Integrity, Availability	Organisational: A manager may reduce or remove access rights of any employee at any time without preliminary notice.
19	Electronic	Any	Transmission	Uncontrolled	Confidentiality, Integrity	Technical: IT4U to ensure that data in transit between Translate and cloud provider are protected (network protection, data encryption)
20	Paper	Confidential	Processing	Controlled	Confidentiality	Legal: The terms and conditions of employment must cover the responsibility for unauthorised access to *Confidential* information.
21	Electronic	Confidential	Storage	Partially Controlled (Cloud Provider)	Confidentiality	Legal: A contractual agreement with a cloud provider to cover the protection of confidentiality of the information of Translate.
22	Paper, Electronic	Public	Creation	Controlled	Integrity	Human-oriented: A marketing officer to take a training on information security and the use of private/confidential information.

Table 8: Information Security Policy Statements developed during the workshops. Part 4 of 4.

1	1. Form	2. Sensitivity	3. Location	4. State	5. Security Goal	6. Security Countermeasure Type: Description
23	Electronic	All	Storage, Transmission	Any	Integrity, Confidentiality, Availability	Organisational: IT4U to report regular about services provided. The management team of Translate to review the reports.
24	Paper	Proprietary	Transmission	Uncontrolled	Authenticity/ Trustworthiness	Organisational: The receipt of a translated document must be sent from an email addresses a customer a has registered with Translate or by a letter signed by a customer. Telephone calls must not be accepted as confirmations.
25	Electronic	Restricted Sharing, Confidential	Transmission, Storage	Uncontrolled	Integrity, Confidentiality	Technical: All information is a USB stick must be encrypted.
26	Electronic	Proprietary, Restricted Sharing, Confidential	Processing	Uncontrolled	Integrity	Human-oriented: Employees must be provided with a training regarding use of social networks. The discussion of customers or job-related matters on social networks are strictly forbidden.
27	Paper	Confidential	Storage	Partially Controlled	Confidentiality	Organisational: An employee may take confidential documents out of the office only with a consent of a manager. The document must not be left unattended at any time and must be kept in a safe or locked container.
28	Electronic	Restricted Sharing	Processing	Partially Controlled	Availability	Technical: Use continuous backup software (e.g. FileHamster) when working on a local machine.

A.10 Evaluation of the RMIAS. Questionnaire

About the respondent:

1. Do you have any experience in Information Security, Information Assurance or related domains? How many years of experience do you have?

2. Does your experience come from practice or research?

3. What is your particular area of interest/responsibility?

The Reference Model of IAS is evaluated against eight criteria: Simplicity, Accuracy, Scope, Systematic power, Explanatory power, Reliability, Validity, and Fruitfulness.

Please answer below the questions related to each criterion.

(Criteria 1) **Simplicity** - among models equal by other parameters the preference is given to the simpler model;

4. Are the elements of the Model simple?

5. Are the relationships between the elements simple? (The relationships are illustrated by arrows.)

(Criteria 2) **Accuracy** - a model, the elements it encompasses and the interrelationships between the elements should be accurate and explicit;

6. Are the classifications included in the model accurate (the information taxonomy, the set of security goals and the types of security countermeasures)?

7. Are the interrelationships between the elements of the model accurately described?

(Criteria 3) **Scope (Completeness)** - a model should cover the broad scope of the domain and should not overlook the essential concepts;

8. Does the model include all elements/concepts essential for the IAS domain? If, in your opinion, there are some essential, but missing from the model elements/concepts, please, name them.

9. Does the model include any elements that are not relevant to the IAS domain?

(Criteria 4) **Systematic power** - a model should help to organise concepts and relationships between them in a meaningful systematic way;

10. Does the model organise elements of the IAS domain and relationships between them in a structured, systematic way?

(Criteria 5) **Explanatory power** - a model should assist with explaining and predicting phenomena;

11. Might the Model assist with explaining (tracing back) and predicting issues related to IAS?

(Criteria 6) **Reliability** - the model should be valid in all situations, for which it is designed, and lead to similar understanding when applied by different users;

12. In your opinion, would the model be valid for the majority of business organisations? Are there any industries or types of organisations where the model would not be applicable (explain your opinion)?

(Criteria 7) **Validity** - the model should provide valid representations and findings;

13. Would the methodology embodied into the model lead to valid results (e.g. comprehensive security policies, correct prediction of InfoSec issues, meaningful tracing back of security breaches)?

(Criteria 8) **Fruitfulness** - desirably, the model should suggest research problems.

14. Does the model provide a convenient structure for framing the existing research? How would you position your area of research/practice using the model?

15. Could the model assist with pointing out the gaps in the existing research/practice?

A.11 Evaluation of the RMIAS. Participants' Profile

Table 9: Participants' Profiles

Resp. No	Date	Exper. (years)	Nature of experience	Area of expertise
1	13.12.2012	6	Research	InfoSec in a distributed environment, risk assessment and management
2	13.12.2012	7	Research	Privacy-preserving data mining
3	13.12.2012	4	Research	Access control, collaboration in health care
4	26.02.2013	6	Both	Cyber domain
5	26.02.2013	20	Practice	IT architecture
6	26.02.2013	32	Practice	ComSec/InfoSec/IA
7	26.02.2013	3	Practice	IT security
8	26.02.2013	2	Both	InfoSec
9	26.02.2013	3	Practice	InfoSec, IA, fraud detection/investigation
10	26.02.2013	2	Practice	Cyber Security and IA
11	26.02.2013	10	Practice	Defence IT operations
12	26.02.2013	20	Both	Cyber defence
13	26.02.2013	10	Practice	Head of a Forensic Computing Unit in the Police
14	26.02.2013	1	Practice	IA policy
15	3.04.2013	2	Research	Non-functional requirements; hard and soft business goals; business process architecture and associated BPMs
16	3.04.2013	15	Both	Platform and infrastructure security; trusted computing
17	3.04.2013	15	Practice	Product development related data (aircraft, ships, IT systems)
18	3.04.2013	5	Practice	Software development and business analysis
19	3.04.2013	15	Both	Bridging the gap between business process models and system models
20	3.04.2013	3	Research	Information architecture design and information management, object-oriented software engineering
21	24.04.2013	12	Practice	Records manager
22	24.04.2013	9	Practice	Data protection and information security
23	24.04.2013	7	Practice	Core IP, data protection officer, business change manager on the InfoSec Programme
24	24.04.2013	10	Practice	Information system security
25	16.05.2013	13	Practice	Cyber defence and information security
26	30.05.2013	25	Both	Requirements definition; responsibility to clients

A.12 Evaluation of the RMIAS. Transcripts of the Interviews

Respondent 1.

Question 1 : 6 years

Question 2 : Research

Question 3 : InfoSec in a distributed environment, risk assessment and management

Question 4 : Yes

Question 5 : The relationships work well for me. They are as simple as could be.

Question 6 : The classifications encompass everything. All security goals are covered. The only thing that I would suggest is, in addition to sensitivity in the information taxonomy, take into account the purpose of use.

Question 7 : The interrelationships make perfect sense as they flow around.

Question 8 : The collaborative aspect is missing.

Question 9 : All elements are relevant: risk; cost-effectiveness, consistency check etc. In fact, the model summarises a common approach.

Question 10 : The model is very good in providing the structured approach in terms of each dimension and in terms of continuous workflow.

Question 11 : Due to the changing nature of a collaborative environment it is very difficult to predict something regarding security. Security audit based on the model may give some level of traceability. The model could be used retrospectively, to trace back security incidents, to see where things went wrong. But to predict will be very difficult. The model may be used for security improvements as overall process, and to certain extent for auditing and monitoring the environment.

Question 12 : The model is suitable for the military environment. It may be applied to many organisations. For smaller organisations (e.g. sole-traders) it may be more difficult to adopt the model because of the time-consuming nature of this type of activity and a need for well-documented processes and policies. Larger organisations, obviously, may much easier spare time and effort on the model consideration and application. Larger organisations may use the model for accreditation purposes in order to define a security status of small organisations.

Question 13 : I assume you could derive valid policies using the model. In fact, validity could only be tested through a careful real case study. Documentation is very important. Interesting to see, how valid it will be for the collaborative environment

Question 14 : Certainly, the model could help with framing the research as an overlay of the dimensions. My research is at the overlay of (1) confidentiality and technical security mechanisms and (2) availability and organisational mechanisms (e.g. processes).

Question 15 : The model could certainly point out the gaps. The location parameter is particularly interesting in the cloud environment. It is interesting to see how location of information is covered from the legal

and organisational side.

Respondent 2.

Question 1 : 7 years

Question 2 : Research

Question 3 : Privacy-preserving data mining

Question 4 : Yes

Question 5 : The top arrow refers to a category of information. It is not clear what is meant by a category of information.

Question 6 : The list of security goals is comprehensive. I have a concern about the forms of information. There may be some additional leafs in this branch.

Question 7 : The link between the first and the second dimensions is not clear.

Question 8 : The model is complete. Its completeness comes from the security goals dimension and the combination between the security goals and the information taxonomy. Further, the completeness of the model may be proved by a comparison with the other models.

Question 9 : All elements are relevant.

Question 10 : The model has a clear structure.

Question 11 : The model may be used for explanation and prediction, but it should be accompanies by more detailed explanation and examples of use.

Question 12 : The model is applicable to any organisation which has information assets. I can see how the model may be applied in the medical environment. I cannot think of any counterexamples.

Question 13 : The model will lead to valid results, but before its application a user should extend a structure of security mechanisms (develop an exhaustive list of security mechanisms for a specific organisation).

Question 14 : I can easily map my research onto the model. I would say that my research concentrates on how privacy could be achieved by technical security countermeasures.

Question 15 : The model could give a hint, if it is used in addition to the literature survey.

Respondent 3.

Question 1 : 4 years

Question 2 : Research

Question 3 : Access control, collaboration in health care

Question 4 : To some extent, if the elements are explained.

Question 5 : To some extent, if relationships are explained

Question 6 : Yes

Question 7 : Yes

Question 8 : Yes

Question 9 : No

Question 10 : Very much, yes.

Question 11 : Yes, to some extent.

Question 12 : Thinking from a patient-centric-care point of view, not all security goals may be necessary. In the healthcare domain, availability (in timely manner) is dominant.

Question 13 : Yes

Question 14 : Definitely, yes.

Question 15 : Yes

Respondent 4.

Question 1 : 6 years

Question 2 : Both

Question 3 : Cyber Domain

Question 4 : Yes

Question 5 : They seem to be, but without applying in practice I am not sure.

Question 6 : Not sure, I would like to use in a real environment to decide.

Question 7 : I would like to use in a real environment to decide.

Question 8 : Not sure, the risks that feed into the security goals to identify possible issues to help populate the table. How? (Does the model help you think about the scenarios to work through). What is a completeness check? Is it when you have 1800 rows or could it be done in less? Why?

Question 9 : No

Question 10 : Yes, as long as it is used correctly.

Question 11 : Not sure, back to the completeness issues: how do you know when all issues have been identified? How would new issues be captured? Model used as a one-off or in an iterative approach?

Question 12 : I think the model would be valid for the majority of organisations, only the level/scale of data would vary, depending on the size of organisations and their domain area.

Question 13 : I think it depends on who is using/implementing the model. The level of detail plus results will depend on the knowledge of the person/people applying it.

Question 14 : No answer

Question 15 : No answer

Respondent 5.

Question 1 : 20 years

Question 2 : Practice

Question 3 : IT architecture

Question 4 : No, the development life cycle is too abstract.

Question 5 : It is not clear or intuitive in terms of the flow of the model. The risk analysis, cost-effectiveness and consistency statements don't seem to connect.

Question 6 : Not sure about the terms, such as security goals as opposed to attributes or characteristics.

Question 7 : No, it requires a supporting narrative. Looks like four models which can be linked.

Question 8 : The model needs to address more explicitly risk analysis and user cases/scenarios.

Question 9 : No

Question 10 : Yes, but it needs explanation.

Question 11 : Not sure, I understand it well enough to answer this question.

Question 12 : Possibly

Question 13 : Possibly, but it could produce too detailed analysis.

Question 14 : No answer

Question 15 : No answer

Respondent 6.

Question 1 : 32 years

Question 2 : Practice

Question 3 : ComSec/InfoSec/IA

Question 4 : They are simple. A very easy way of expressing requirements to key stakeholders.

Question 5 : Yes

Question 6 : Yes, and potential to change/adapt depending on the company.

Question 7 : Yes

Question 8 : Yes

Question 9 : No

Question 10 : Yes

Question 11 : Potentially. It is IS Risk Analysis mere.

Question 12 : Yes. No.

Question 13 : Yes

Question 14 : No answer

Question 15 : No answer

Respondent 7.

Question 1 : 3 years

Question 2 : Practice

Question 3 : IT security

Question 4 : Yes

Question 5 : Yes

Question 6 : Yes

Question 7 : Yes

Question 8 : Yes

Question 9 : No

Question 10 : Yes

Question 11 : Yes.Prediction primarily.

Question 12 : Possibly more suitable for smaller businesses with less resources.

Question 13 : Yes

Question 14 : No answer

Question 15 : No answer

Respondent 8.

Question 1 : 2 years

Question 2 : Both

Question 3 : InfoSec

Question 4 : Yes

Question 5 : Yes

Question 6 : Yes

Question 7 : The top left quadrant's relationship with adjacent quadrants was not overly clear to me.

Question 8 : Yes

Question 9 : No

Question 10 : Yes

Question 11 : Possibly.

Question 12 : I am not aware of any organisations where the model would not be suitable.

Question 13 : Difficult to define at this point. Appears likely.

Question 14 : No answer

Question 15 : No answer

Respondent 9.

Question 1 : 3 years

Question 2 : Practice

Question 3 : InfoSec, IA, fraud detection/investigation

Question 4 : Yes

Question 5 : Yes

Question 6 : Yes. Not always appropriate to each business (e.g. document classification)

Question 7 : Yes

Question 8 : Not sure

Question 9 : No

Question 10 : Yes

Question 11 : Yes

Question 12 : A world, I think.

Question 13 : Yes, as shown through the case-study.

Question 14 : No answer

Question 15 : No answer

Respondent 10.

Question 1 : 2 years

Question 2 : Practice

Question 3 : Cyber Security and IA

Question 4 : Yes

Question 5 : Yes

Question 6 : Ok with me, but could be argued.

Question 7 : Yes

Question 8 : Yes

Question 9 : No

Question 10 : Yes

Question 11 : Yes

Question 12 : Yes

Question 13 : No sure

Question 14 : No answer

Question 15 : No answer

Respondent 11.

Question 1 : 10 years

Question 2 : Practice

Question 3 : Defence IT operations

Question 4 : Following the explanation, the model is simple. However, its rather comprehensive approach possibly detracts from the optimum level of simplicity.

Question 5 : I believe the relationship within the elements are simple, but they do not necessarily flow between elements logically.

Question 6 : They are thorough as a synthesis of many other models.

Question 7 : Yes

Question 8 : Yes

Question 9 : No

Question 10 : Yes

Question 11 : Not sure

Question 12 : Yes, it is a good basis for developing an IS security policy.

Question 13 : Yes

Question 14 : No answer

Question 15 : No answer

Respondent 12.

Question 1 : 20 years

Question 2 : Both

Question 3 : Cyber defence

Question 4 : It depends on the resources that the enterprise has to understand the model. For an SME, I'd suggest no.

Question 5 : Yes

Question 6 : Yes

Question 7 : Yes

Question 8 : The security design stage should emphasise a human factor.

Question 9 : No

Question 10 : Difficult to assess at this stage, it requires further use.

Question 11 : Yes

Question 12 : No, not for SME.

Question 13 : Depends on the training and understanding of the practitioner.

Question 14 : No answer

Question 15 : No answer

Respondent 13.

Question 1 : 10 years

Question 2 : Practice

Question 3 : Head of a Forensic Computing Unit in the Police

Question 4 : Yes, it appears clear and easy to implement.

Question 5 : Yes

Question 6 : Yes

Question 7 : Not sure

Question 8 : Yes

Question 9 : No

Question 10 : Yes

Question 11 : No

Question 12 : Not sure

Question 13 : Yes, if it is applied properly

Question 14 : No answer

Question 15 : No answer

Respondent 14.

Question 1 : 1 year

Question 2 : Practice

Question 3 : IA policy

Question 4 : Yes

Question 5 : Not sure about the lifecycle.

Question 6 : Yes, but the vocabulary is quite academic. E.g. Information Taxonomy may not be very meaningful to people who have not seen the IAS model before.

Question 7 : Yes

Question 8 : Yes

Question 9 : No

Question 10 : Yes

Question 11 : Yes

Question 12 : Not sure

Question 13 : Yes, if there is simple and clear explanatory notes on how to use the model.

Question 14 : No answer

Question 15 : No answer

Respondent 15.

Question 1 : 2 years

Question 2 : Research

Question 3 : Non-functional requirements; hard and soft business goals; business process architecture and associated BPMs

Question 4 : Yes

Question 5 : Yes

Question 6 : Yes

Question 7 : Yes, but I would prefer if you could explicitly illustrate the starting point of the model. In the security life cycle dimension.

Question 8 : Yes, at this stage they are all included.

Question 9 : No

Question 10 : Yes. Also it will be a good idea if you could implement this work in a form of a catalogue and with associated input and outcome for each stage.

Question 11 : Yes. I think your model will assist in predicting issues and tracing them back. Thanks to the goals, which occupy the third dimension of your model. For example, goals assist in detecting gaps.

Question 12 : I think, this model is promising and valid for many domain-independent organisations. At the

current stage, I can say yes for most organisations. This answer is not because I know many organisations that look for this kind of model, yet it addresses most required perspectives. In order to make it valid for the majority of business organisations, you must deliver it in a way flexible to receive and welcome changes from experts in the field to adapt it with their needs.

Question 13 : I am not sure if your model has included the risk mitigation countermeasures which are different from security countermeasures I can't say the model will lead to valid results until it is evaluated using case studies. The model will attract the experts, if it is comprehensive and easy to apply.

Question 14 : Yes it does. My research work aims to align business process architectures with business goals, which they might be hard and soft goals. In fact, the security is one of the most required soft goals in a Business/IT organisation. My work fits very well with your model and particularly with the first, second and fourth stages. I am not sure how would it fit with the third stage, which is the information taxonomy. However, we can benefit from your model and it fitness with my work using the three aforementioned dimensions in order to fit it with the information taxonomy.

Question 15 : Yes definitely. My research work possesses this advantage in detecting gaps. And thanks again to the goals that motivate the derivation of other stages. Therefore, by using your model you may be able to detect unrequired and/or missing business-oriented objects in an organisation.

Respondent 16.

Question 1 : 15 years

Question 2 : Both

Question 3 : Platform and Infrastructure Security; Trusted Computing

Question 4 : Yes

Question 5 : Yes

Question 6 : It is rather static, but comprehensive (good).

Question 7 : Not quite

Question 8 : The notion of goal is not quite clear, is it applicable to assets (information) or to a person, organisation.

Question 9 : Privacy and Auditability could be argued. (Good you have included them anyway.)

Question 10 : Yes, but the process of applying the model is not quite clear.

Question 11 : Not sure

Question 12 : Good for any type of organisation.

Question 13 : Not sure

Question 14 : The model provides a useful structure particularly with respect to encouraging users to consider forms and states of information. The subdivision of security countermeasures looks useful.

Question 15 : Yes, due to the way the model splits out the different dimensions.

Respondent 17.

Question 1 : 15 years

Question 2 : Practice

Question 3 : Product development realted data (aircraft, ships, IT systems)

Question 4 : Yes

Question 5 : Not quite. Seemingly yes, but the relationship are in reality quite complex and may vary depending on the context.

Question 6 : Yes, but of course depend of the definitions used.

Question 7 : Accurate, but incomplete as the relationship between components of different domains of the model are not visualised in detail.

Question 8 : It seems quite complete, but depending on the context there may be different ways to categorise matters.

Question 9 : No

Question 10 : Yes

Question 11 : Yes

Question 12 : It could be adopted by many companies generally, but in some specific context, different definitions, more details may be included.

Question 13 : It could contribute to comprehensive security policy.

Question 14 : No answer

Question 15 : No answer

Respondent 18.

Question 1 : 5 years

Question 2 : Practice

Question 3 : Software development and business analysis

Question 4 : Yes

Question 5 : Yes

Question 6 : Yes

Question 7 : Yes

Question 8 : Yes

Question 9 : No

Question 10 : Yes. I imagine an auditor would be very pleased to see all potential 1800 statements accounted formally.

Question 11 : Yes

Question 12 : Yes, but of course, as you said, classifications are sometimes "more than one".

Question 13 : I don't know

Question 14 : No answer

Question 15 : No answer

Respondent 19.

Question 1 : 15 years

Question 2 : Both

Question 3 : Bridging the gap between business process modelling and system models

Question 4 : Yes. They appear to be simple at the coarse or more abstract level.

Question 5 : Not seen as simple because the relationships could carry different meanings to different people.

Question 6 : Not clear.

Question 7 : Not clear.

Question 8 : The coverage, based on the cited literature, seems highly covering, but it is not guaranteed.

Question 9 : No

Question 10 : Yes, being complex it needs further work for the appreciation in industrial settings.

Question 11 : Yes, good traceability foreseeing/backwards.

Question 12 : Not an easy question.

Question 13 : Yes

Question 14 : Not sure.

Question 15 : Yes, I believe so. This is due to the way the model splits out the different dimensions of InfoSec and further splits these down prompting thought on each individual aspect of information security. The model starts a useful dialogue about the limitations of the CIA-triad.

Respondent 20.

Question 1 : 3 years

Question 2 : Research

Question 3 : Information Architecture Design and Information Management, Object-Oriented Software Engineering

Question 4 : Elements of model are simple, but the difficulty lies in how to show them (I think!). The model needs to be viewed from other perspectives for identifying its simplicity. I mean that if the model is four dimensional, can I present it as a series of three dimensional projections that progress over the fourth dimension?

Question 5 : I struggled to understand the relationships in the initial part of your presentation, but with on-going discussion, it became somewhat clearer. I still maintain a top-down view of the organization and find information security and assurance (IAS) to be translated down from business strategy to business processes and information itself. You have probably shown me the inside-out view where IAS stands in the organization and how IAS sees the organisation outwards.

Question 6 : Yes. The classification are accurate and they make sense!

Question 7 : No. This is where I think the problem is. A lot of it may be related to how we view the

organisation and how we place the IAS in it.

Question 8 : Yes

Question 9 : No

Question 10 : Yes. May be a change of a view-point on IAS could initiate change in the structure of the model!

Question 11 : I do not know, to be honest! Although the presented view-point of the model is different from my own, it may still be able to explain or predict IAS issues, but this would also depend on security analytics produced regularly for information.

Question 12 : Not sure

Question 13 : Maybe. Only case study will be helpful in determining that.

Question 14 : Not sure. My research will interface with IAS within Enterprise Architecture domain.

Question 15 : I am not correctly positioned for answering this at the moment due to a lack of knowledge on this!

Respondent 21.

Question 1 : 12

Question 2 : Practice

Question 3 : Records Manager

Question 4 : I think that the model, with regards to the dimensions is fairly simple to understand. I don't think it would be as easy to implement because it will highlight such a high number of risks.

Question 5 : "(Yes) Yes, although I'm not sure that the description on the right hand side of the model is accurate as an organization does not analyse the risks when they set their security goals but afterwards once they compare their information taxonomy against their security goals.

Question 6 : Yes, although a high number of risks are identified if information is classified by form and sensitivity, but not by type of content. E.g. email is a form, but can be used to carry many different types of messages of varying types and/or sensitivities.

Question 7 : No, as mentioned above I don't think the interrelationship between the taxonomy and security goals quarters is accurate. I also think that in practice some analysis of the risks would be needed as well as the considerations about cost-effectiveness. Even with the prioritised security goals you will still have a very large list of risks and will need to identify which ones to tackle first.

Question 8 : Yes

Question 9 : I think the further subdivision of the core security goals (integrity, availability and confidentiality) may assist people in understanding what the element entail, but may not add anything as separate goals in their own right.

Question 10 : Yes, although as mentioned above I'm not sure about the relationship between the two right hand boxes and the process between the bottom two boxes.

Question 11 : I think in order to assist there would need to be an element of probability assessment in the risk analysis stage.

Question 12 : I think that the model could be used in various settings..

Question 13 : I think to get an organisation to buy into tackling information security there would need to be some realistic risk analysis and probability assessment.

Question 14 : No answer

Question 15 : No answer

Respondent 22.

Question 1 : 9 years

Question 2 : Practice

Question 3 : Data Protection and Information Security

Question 4 : Yes

Question 5 : They are presented as such, but in reality that is not necessarily how it works

Question 6 : Yes

Question 7 : We debated the issue of whether you can classify a document before knowing your security goals, plus the risk assessment aspect continues when selecting security mechanisms (not just cost-effectiveness), rather than at the security goals stage only.

Question 8 : The role of risk assessment while selecting security countermeasures must be highlighted.

Question 9 : No

Question 10 : Yes

Question 11 : I don't think the model works particularly well.

Question 12 : I don't think this model works well for organisations who have many different types of form, sensitivity, locations, states and security goals. The permutations table gets far too large to be helpful and there is no consideration of risk assessment and risk appetite in the way the method was applied.

Question 13 : To use it to plan going forward no. I don't think so because of the lack of risk assessment incorporated into the application of the model in practice. A policy is more than the list of finalised security goals.

Question 14 : No answer

Question 15 : No answer

Respondent 23.

Question 1 : 7 years

Question 2 : Practice

Question 3 : Core IP, Data Protection Officer, Business Change Manager on the Information Security Framework Programme

Question 4 : Yes, the elements are reasonably self-explanatory and straight forward to understand. One comment I have is that visually the diagram gives the impression that you would complete the contents of each quadrant (so to speak) before moving onto the next. However the security development life cycle is not

something you would ""complete"" before moving onto the information taxonomy dimension. In practice, when carrying out security requirements elicitation you would ""Consider every stage of information"", ""Prioritise security goals"", and ""Select security countermeasures"" before moving to the security design stage in the development life cycle. I am not convinced the development life cycle sits as a quadrant within the diagram and should perhaps sit centrally or outside the diagram. Steps 1,2 and 3 in the security development life cycle are informed by information taxonomy, security goals and security countermeasures, so it feels incongruous to have them in a flow.

Question 5 : Yes, the relationships are simple.

Question 6 : Yes. However, as discussed within the workshop, the nuance differences between some of the security goals and the standard trio of confidentiality, availability and integrity are sometimes hard to see, e.g. trustworthiness and integrity.

Question 7 : Yes

Question 8 : Yes, just add insurance as a security countermeasure under the heading Legal.

Question 9 : No

Question 10 : Yes

Question 11 : Yes. Using the model, you would be able to trace back logically and demonstrate how an element of information security had been missed.

Question 12 : I am not aware of an organisational type for which the model would not be relevant.

Question 13 : Yes. However the process as attempted within the workshop seemed resource intensive prompting you to consider 5 states for each form of information e.g. account registration emails the sensitivity of that information and the location. Each of these then has 8 security goals to be assessed for applicability. This leads to an exhaustive process generating a considerable amount of data. Whilst this approach would cover every possible angle it would not seem an efficient use of resources.

Question 14 : No answer

Question 15 : No answer

Respondent 24.

Question 1 : 10 years

Question 2 : Practice

Question 3 : Information system security

Question 4 : Yes

Question 5 : Yes

Question 6 : As stated, the RMIAS is a "generic abstraction", so in that respect overall it is OK. Although I feel the model diagram does not properly demonstrate the requirement for information security to be an integral part of the information system development from inception to decommissioning.

Question 7 : I consider that the top arrow should read "The beginning of the information system life cycle" or at least "From an early stage ..." to emphasise the importance of IAS being an integral part of the information system life cycle. The Cost-Effectiveness sub label of the Select Security Countermeasures arrow might be

misinterpreted as cost-benefit. Perhaps the phrase "cost-effectiveness analysis" would be more specific.

Question 8 : As a generic abstraction it appears to cover the principal areas I would expect.

Question 9 : No

Question 10 : Yes

Question 11 : At this stage, I am not certain. I would need to see its application across a wide range of organisaions of different size and type.

Question 12 : Where a single organisation is involved it might be a useful tool. The more interesting application would be in a multi-organisation joint venture/project say Higher Education, Health Service and Pharmaceutical Company to see if the methodology can produce a policy to meet all stake-holders requirements.

Question 13 : At this stage I am not certain. I can see elements such as the information taxonomy and security goals could be useful tools when introducing the subject to non-InfoSec/IT people.

Question 14 : No answer

Question 15 : No answer

Respondent 25.

Question 1 : 13 years

Question 2 : Practice

Question 3 : Cyber Defence and Information Security

Question 4 : Yes

Question 5 : Yes

Question 6 : Yes, but I am not so happy with the taxonomy part though. This part is, in my opinion, relatively weak.

Question 7 : Yes

Question 8 : Yes

Question 9 : No, but I would estimate that the classification thing is probably not applicable to 90% of the commercial entities out there, even if they could greatly benefit from it.

Question 10 : For the elements: yes. For the relationships: no.

Question 11 : Not to me

Question 12 : It is applicable. I cannot think of any exceptions. Of course depending on the organisation the one or the other dimension might prevail.

Question 13 : I do not think that comprehensive security policies can be deducted from the model. I also do not think that it can predict issues since it does not consist of any instructions concerning the actual implementation on a managerial level. Of course, if people oversee a complete dimension then there is an issue.

Question 14 : No answer

Question 15 : No answer

Respondent 26.

Question 1 : 25 years

Question 2 : Both

Question 3 : Requirements definition; responsibility to clients

Question 4 : No! But then it is a complex area.

Question 5 : Simple to understand, but the "nature" of the relationships may be complex.

Question 6 : Seem adequate, but I wonder whether responsibility should also be included in the "information taxonomy" area.

Question 7 : Seem to be ok.

Question 8 : I wonder whether the definition of business goals should be more explicit; this comment arises from the consideration of ICT as a ""serving system"", and the underpinning idea that it is necessary to understand the ""system served"".

Question 9 : I don't believe so.

Question 10 : I am not convinced it does. There are a number of reasons for my view, not least of which is the lack of "systemic understanding" among managers. I fear the arrows in the model will be interpreted as a time dependency, rather than a logical interdependency.

Question 11 : Possibly, if it is seen as demonstrating a logical dependency.

Question 12 : Because it is a reference model, its principles should of course be widely applicable. I would need to consider more carefully whether certain types of service provider would find it useful. For example, I wonder if it enables a cloud service provider to distinguish its responsibilities from those of its clients. I would hope that a model such as this would help me to define contractual requirements, but (and I do not have particular experience to guide me here) I cannot see how it would help me in this regard.

Question 13 : I can see how it would inform practitioners of particular methodologies, and that may be good enough. However, I believe that the fashion in IT is to minimise the need to "think" and the model requires users *to think* (probably, based on substantial knowledge and experience); anything that requires thinking implies, to my mind, that a range of answers may be derived. Perhaps your question should have asked whether the model can lead to "defensible" (rather than valid) results, in which case I would have offered the answer of a tentative "yes".

Question 14 : I think it could help assess competing requirements "methodologies" (i.e. do "stories", or "SSM", or "personas" allow effective use of the model). It has some value as a check-list for consultancy practice.

Question 15 : The model could usefully indicate a need for more knowledge. For example, given the need to consider cost-effectiveness in selecting technology, do we know what the value of, say, cryptography is? The model could be considered as defining a research agenda.

A.13 Evaluation of the RMIAS. Interviews Summary

Table 10: The RMIAS Evaluation. Interviews Answers Summary.

Question	Answer	Responses
Q4. Simplicity. Elements.	Yes	22
	No	4
	Not sure	0
Q5. Simplicity. Relationships.	Yes	17
	No	7
	Not sure	2
Q6. Accuracy Elements.	Yes	18
	No	5
	Not sure	3
Q7. Accuracy Relationships.	Yes	14
	No	9
	Not sure	3
Q8. Completeness.	Yes	18
	No	5
	Not sure	3
Q9. Elements Relevance	Yes	24
	No	2
	Not sure	0
Q10. Systematic Power	Yes	22
	No	3
	Not sure	1
Q11. Explanatory Power	Yes*	17
	No	3
	Not sure	6
Q12. Reliability. Wide Applicability.	Yes	16
	No**	5
	Not sure	5
Q13. Validity. Valid Results.	Yes***	16
	No	2
	Not sure	8
Q14. Fruitfulness. Research Structuring. ****	Yes	6
	No	0
	Not sure	2
Q15. Fruitfulness. Gaps Pointing. ****	Yes	7
	No	0
	Not sure	1

Note: * - includes 10 respondents who answered "Yes" and 7 respondents who answered "Yes, with some reservations"; ** - refers the participants who pointed out at the limited applicability of the RMIAS; *** - includes 11 respondents who answered "Yes" and 5 respondents who answered "Yes, with some reservations"; **** - only 8 participants were invited to answer this question.

A.14 Integration of IAS into BPM. Other Related Work

Reviews of research related to the integration of IAS into BPM

The integration of security concerns into business process models is a dynamic area of research. Many extensions which are reviewed further in this section emerged after 2010, the year when this research project started. The research in this field is also actively examined and analysed as demonstrated below.

In 2006, the analysis of business process management methodologies resulted in a roadmap for Secure Business Process Management [29]. This roadmap, among other factors, pinpointed the importance of integrated modelling of business processes and security. Integrated modelling was said to enhance transparency and awareness, and to help aligning workflow systems with security requirements.

In 2009, the detailed survey of nine attempts to integrate security and risk aspects into business process management was presented [175]. This survey identified several gaps in the research. Two of them, which are relevant to this thesis, were (1) the need to extend a list of security goals and (2) the need to improve business process modelling notations for security modelling.

In 2010, the representation of security in business process models was examined and summarised [176]. The paper demonstrated that a range of security goals and countermeasures, including concepts such as privacy, documentation, authorisation, access control, separation of duties etc. in addition to the CIA-triad are addressed by security extensions. Two challenges facing research on security in business process models were outlined: (1) the development of a semantics covering all key security concepts and (2) the representation of this comprehensive semantics in "*an expressive yet intuitive manner*" [176].

In 2010, a review and analysis of the research attempts to integrate risk and business process modelling was carried out [238]. As a result of this analysis, a reference model of a risk-aware business process was proposed. This model included four risk elements: threat, detection measures, countermeasure and recovery measure.

In 2013, the syntax of six BPMN security extensions was analysed [177]. A set of ten security concepts was extracted from the extensions examined. Then, it was evaluated how well the audience, unfamiliar with the security extensions, could map the symbols proposed in the extensions with the concepts the symbols illustrate. This analysis proposed two recommendations for the design of the syntax of security notations: (1) the use of scientific principles and (2) the involvement of users. It was also recommended to provide training on security to individuals involved in experiments.

In 2014, a detailed analysis of 275 papers, published between 1993 and 2012 and related to security in Process-Aware Information Systems (PAIS), was conducted and presented in [178]. The security in PAIS was confirmed to be an interdisciplinary field of research which requires the knowledge of a broad range of

disciplines. Echoing one of the problems stated and addressed in this thesis, the lack of an agreed understanding of the security in PAIS was pointed out : "*an agreement on a common terminology or requirements on security in PAIS as well as widely accepted guidelines or models are missing, although, there is a general understanding that security in PAIS is a key challenge*" [178]. The analysis showed that authorisation and access control are the security requirements which receive the most attention in PAIS.

The development and standardisation of security terminology and of the approach to security in PAIS was designated as a research challenge in the field [178]. Another challenge was to extend beyond the technical orientation of the approach to security in PAIS and move towards the human-orientation. A need for an holistic approach to security was articulated [178], supporting the argument of this thesis and justifying the relevance of the proposed in this thesis solution.

In 2014, an analysis of eleven research proposals to extend UML and BPMN for security modelling was undertaken [179]. This analysis mainly concentrated on the extensions developed for the SOA environment. The analysis confirmed that the proposals address different sets of security goals and highlighted that many proposals are text-based, while fewer suggest graphical annotations [179].

In 2014, the thorough analysis of twenty seven distinct approaches to the integration of risk into BPM was presented in [180]. The analysis indicated that the proposals suggest the integration of risk management into UML, Event-driven Process Chain modelling languages and Entity Relationship diagrams, and concluded that, although many proposals exist, there is still room for multiple improvements.

Other Related Literature

There are many extensions for BPMN which address modelling of non-functional requirements [239, 240, 241]. These extensions address security only superficially among other factors such as performance, regulatory compliance, reliability, the quality of user interactions etc. These extensions were not included in the detailed analysis because the vocabulary they use and the context of work make the comparison with the security extensions hard to undertake.

Many proposals exist which extend UML for modelling of different security aspects [242, 243, 244, 245, 246, 247]. Security in use-case diagrams is addressed in [249, 248, 250].

In [251], a Risk-Oriented Process Evaluation (ROPE) methodology is introduced. The ROPE allows simultaneous optimisation of business processes in terms of efficiency and security. The methodology is based on the Security Ontology [252, 68]. The Security Ontology is a conceptual schema of IT security, based on the NIST security relationship model. The authors adopt security objectives (availability, reliability, safety, confidentiality, integrity, maintainability) from [224], which concentrates mainly on the dependability, rather than security of computing. Therefore, out of the security objectives used in [251] only three,

namely confidentiality, integrity and availability are relevant to security. The approach focuses on IT security and considers IAS as a purely technical issue. However, the paper mentions that the authors plan to extend in the future the Security Ontology with the classification of human resources.

In [19], the Security via Commitments (SecCo) modelling language is introduced. Security requirements are derived based on the objectives and interactions between collaborators. SecCo is a language of a higher level of abstraction than BPMN, it captures business goals rather than processes.

The integration of security aspects into the goal-based development methodology TROPOS is described in [204]. TROPOS, which does not by default embed security modelling elements, is enriched with such elements as security diagram, security constraint, secure dependency, and secure goal, task, and resource.

A.15 Model-Driven Engineering

This section gives a brief introduction to the Model-Driven Engineering (MDE) paradigm. This is required mainly for the understanding of the context of the related proposals examined in Section 5.4 and the difference between these proposals and Secure*BPMN.

Model-driven engineering is a software development paradigm, where software (code) is developed based on a set of domain models as a result of several transformations.

One of the most popular methodologies within the model-driven engineering paradigm is the Model Driven Architecture (MDA) proposed by the Object Management Group [256]. The MDA declares that models of three levels of abstraction shall be designed and transformed sequentially into each other and, finally, into executable code. These three levels, as depicted in Figure 2, are

- Computation Independent Models (CIM) - these are the business models of real-world objects and their behaviour. These models are concerned with the requirements for and environment of a system. CIM are independent of the computation viewpoint. They are developed typically using the vocabulary which is closer to the practitioners of a modelled domain. The business process models, which are considered in this thesis, are CIM;
- Platform Independent Models (PIM) - these are the specification models which describe a system independently from an intended platform. PIM incur a degree of independence as they depict a system at such level of detail which may be implemented using any platform;
- Platform Specific Models (PSM) - these are the implementation models, which describe a system at the level of detail specific to an intended realisation platform.

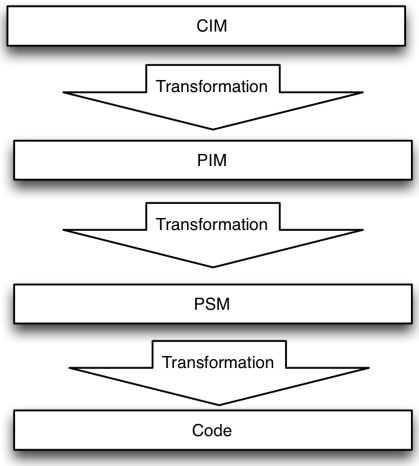


Figure 2: Model-Driven Architecture [257]

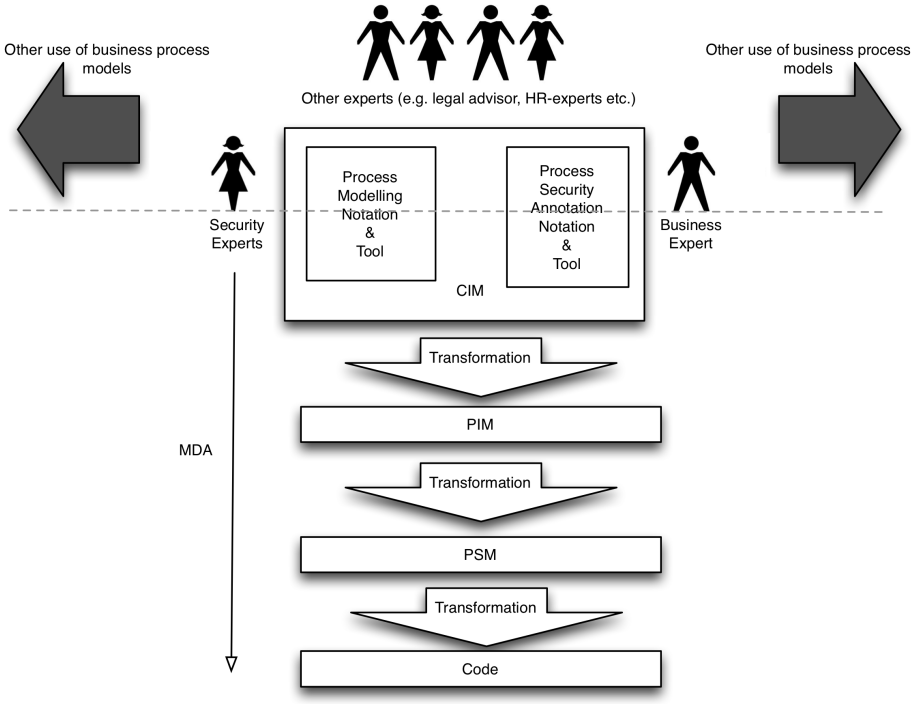


Figure 3: Clarification of the approach to business process modelling adopted in this thesis.

There is also the model-driven security approach which inherits from the model-driven engineering paradigm. This approach, through the integration of security into business process models and, then, via a series of transformations, leads to the generation of executable security configurations [258, 259, 260].

MDE and model-driven security methodologies are software development methodologies and concentrate on software only. However, in this thesis a broader definition of an IS is adopted (Definition 4). In this definition software is said to be only one of six components of an IS. A secure IS is not limited to secure software, other components of the system must adhere to security as well. As mentioned in Chapter 5, business process models may be used for a range of purposes apart from software development. In the context of model-driven methodologies, business process models are used only in order to produce executable code and security configurations.

Figure 3 clarifies the differences between the approach to business process modelling adopted in this thesis and in the model-driven engineering paradigm (and, consequently, in the papers which are written within the MDE paradigm and which are discussed in detail later in this chapter). The MDE paradigm concentrates on the issues below the dashed line, i.e. the transformation of the model of one type into another and the generation of executable code. The security-annotation of business process models at the CIM level only interests the MDE paradigm followers with the view to enable the transformation of business process models into executable code. Also, often within the model-driven security approach, as identified via the analysis of

related work conducted, only the involvement of technical security and business experts is discussed, while ignoring the need to take into account the knowledge of experts of other domains when security-annotating business process models.

This thesis, on the contrary, propose to concentrates on the issues that cluster above the dashed line. While the MDE paradigm considers only the use of business process model for the generation of executable code (the top down direction in Figure 3), this thesis accepts the view that automation is only one of the possible implications of business process models and that business process models may be utilised for others purposes such as, for example, documentation, optimisation, communication, education etc. (shadowed arrows and the right-to-left direction in Figure 3). In this thesis, the need to involve the experts of other domains in security-annotation, in addition to security and business experts, is also acknowledged and addressed.

A.16 Annotation Task (Task 1)

1. Tender Process Description

Translate is a small business which offers a variety of translation services. Translate looks for a new IT service provider and starts a tender process in order to collect competing offers from different IT-service providers.

The BPMN diagram in Figure 4 shows that Translate prepares an Invitation to Tender and sends it to a number of the prospective IT-service providers. On receipt of the Invitation to Tender, a service provider checks the requirements and produces a bid. Then a service provider submits a bid to Translate. On receipt of a bid, Translate registers the bid.

2. Security details of the Tender Process

Translate classifies its information as follows:

- Public: press releases, advertisement emails and brochures, and invitations to tender;
- Proprietary: original customers' documents, translated documents in paper or electronic form;
- Restricted Sharing: financial statements;
- Confidential: salaries, financial reports, audit opinion and reports, tender bids.

An Invitation to Tender is an electronic document which is send to IT service providers by email. A bid is a paper document, which is sent by a bidding service provider to Translate by post.

Completeness and accuracy (Integrity) of an Invitation to Tender has medium criticality for Translate. To ensure integrity of an Invitation to Tender, Translate performs a check of this document before it is sent out. An employee different from an employee who prepared the document ensures integrity of the Invitation to Tender (Four-eyes principle). To prevent one supplier getting the advantage over another by finding out the details of the submitted bids and offering better conditions, the bids are confidential. Therefore, Accountability for the bids registration procedure has high criticality for Translate. There is a legal agreement between employee and Translate about non-disclosure and confidentiality of the details of bids. On the basis of this agreement an employee may be held accountable for the information misuse. At the time of the tender process, there are no contractual relationships between Translate and any of the perspective IT-service providers.

!!!! PLEASE NOTE TASK 1 START TIME NOW !!!!

3. Annotation steps

Please annotate the BPMN diagram in Figure 4 following the steps:

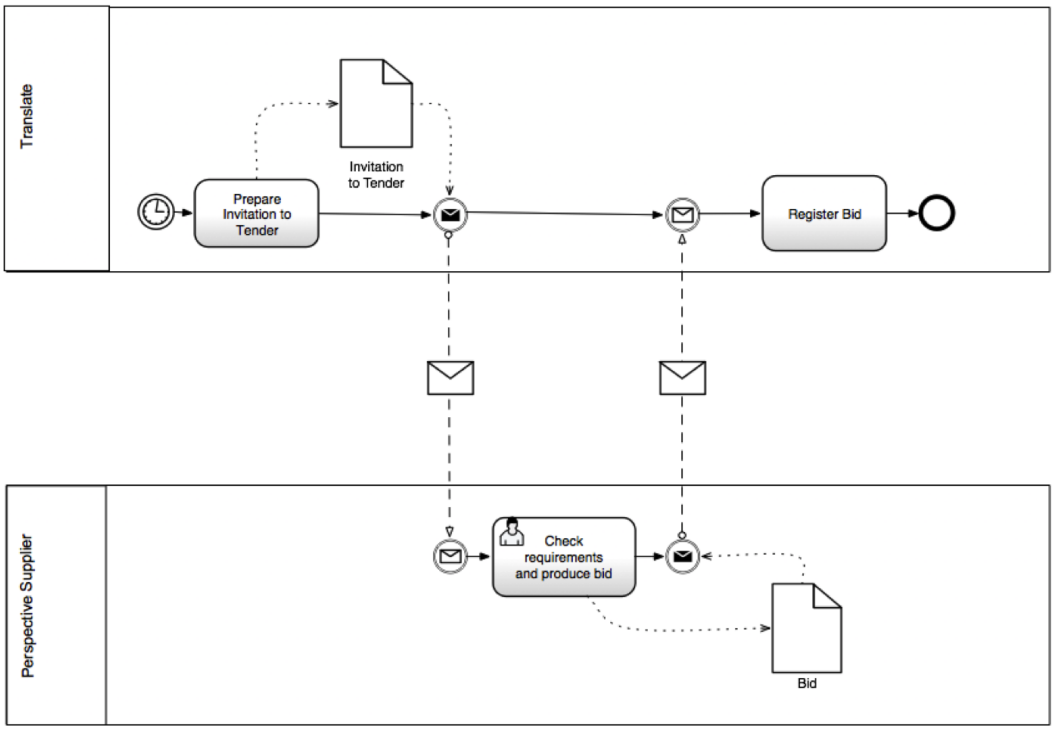


Figure 4: The tender process

1. Set locations for process participants (controlled, partially controlled or uncontrolled);
2. Set access permissions for each participant;
3. Set form and sensitivity for each document;
4. Depict security goals mentioned in the description;
5. Suggest and depict at least one security goal not mentioned in the description.
6. Depict security countermeasure(s) mentioned in the description;
7. Suggest and depict at least one security countermeasure not mentioned in the description.

!!!! PLEASE NOTE TASK 1 END TIME AS SOON AS YOU FINISHED ANNOTATION !!!!

A.17 Annotation Task (Task 1) Marking Scheme

Secure*BPMN Empirical Evaluation. The Annotation Task Marking Schema.

Evaluated Parameter	Max score	Marking rules
Location	2	+1 - Translate is designated as a controlled environment; +1 - Supplier is designated as an uncontrolled environment.
Access Permissions	2	+0.25 - For each (out of 4) sensitivity markers next to the pool name in the pool of Translate; +1 - A Public sensitivity marker next to the pool name in the pool of Supplier (-0.25 for each additional marker).
Information Format	2	+1 - The invitation to tender data object is marked as electronic; +1 - The bid data object is marked as paper.
Information sensitivity	2	+1 - The invitation to tender data object is marked as public; +1 - The bid data object is marked as confidential.
Security Goal	2	+1 - The security goal Integrity is associated with the invitation to tender data object; +1 - The security goal Accountability is associated with the bid data object or the register bid activity..
Criticality of a Security Goal	2	+1 - Integrity has medium criticality (symbol with midium darkness); +1 - Accountability has high criticality (symbol with high darkness).
Security Countermeasure	2	+1 - A security countermeasure "Four-eyes principle" (or "integrity check") appears next to the invitation to tender data object; +1 - A security countermeasure "Non-disclosure Agreement" appers next to the bid data object
Application Rules	2	+ 0.25 - use of a line to associate Secure*BPMN elements with BPMN elements; + 0.25 - use of a correct type of line; + 0.25 - correct position of information form markers; + 0.25 - correct position of sensitivity markers; + 0.25 - security countermeasures accompanied by descriptions; + 0.25 - attachment of a security goal to a variety of BPMN elements; + 0.25 - attachment of a security countermeasure to a variety of BPMN elements; + 0.25 - type of a security countermeasure to correspond with a description.
Understanding	2	+1 - The participant has specified at least one relevant security goal at his discretion; +1 - The participant has specified at least one relevant security countermeasure at his discretion.

A.18 Interpretation Task (Task 2)

Note: The description of the task, diagrams and questions are presented as they appeared in the actual survey.

Interpretation of a security-annotated BPMN diagram (TASK 2) First, you are presented with a BPMN diagram of a process of the translation service provision. Then, you will see the same BPMN diagram annotated with security information. Please examine both diagrams and answer the questions below. You may refer to any notes on Secure*BPMN at any time.

1. This is a BPMN diagram of a process of the translation service provision (Figure 5).

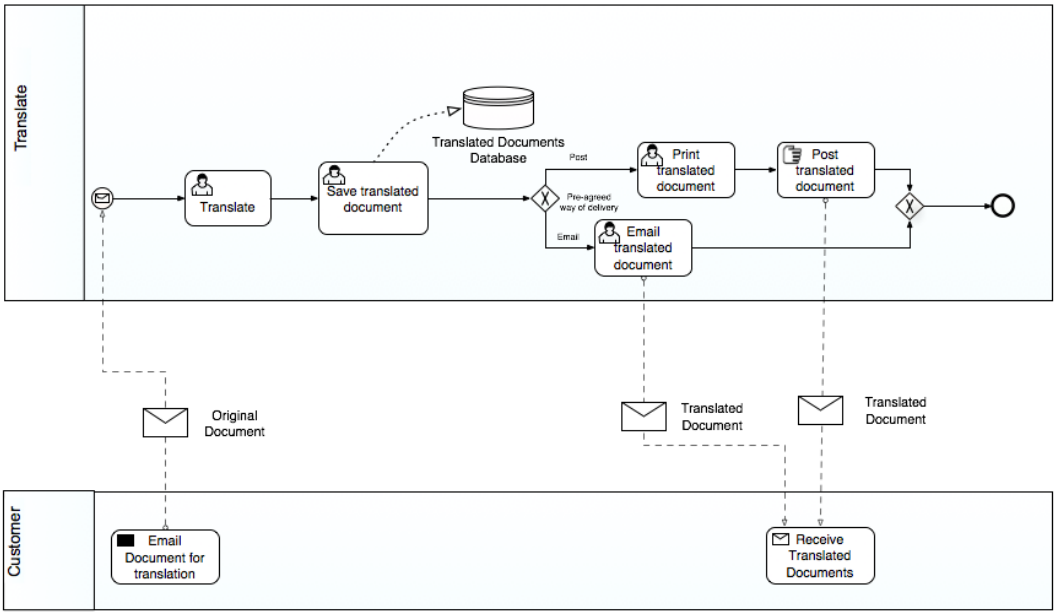


Figure 5: The translation service provision

A customer sends to Translate a document for translation. On receipt of the document, an employee of Translate translates the document and saves a translation in the database of translated documents. Depending on whether customer requested an electronic or a paper copy of the translated document, an employee of Translate will either print and post the document, or will email it to the customer.

2. * ———— PLEASE NOTE the TASK 2 START TIME NOW ————

This is a security-annotated BPMN of the translation service provision process (Figure 6). Please examine the diagram and try to interpret the security annotations.

After examining the diagram, please answer the questions below the diagram.

Q3. This diagram is drawn from the perspective of Translate.

Correct | Not sure | Incorrect

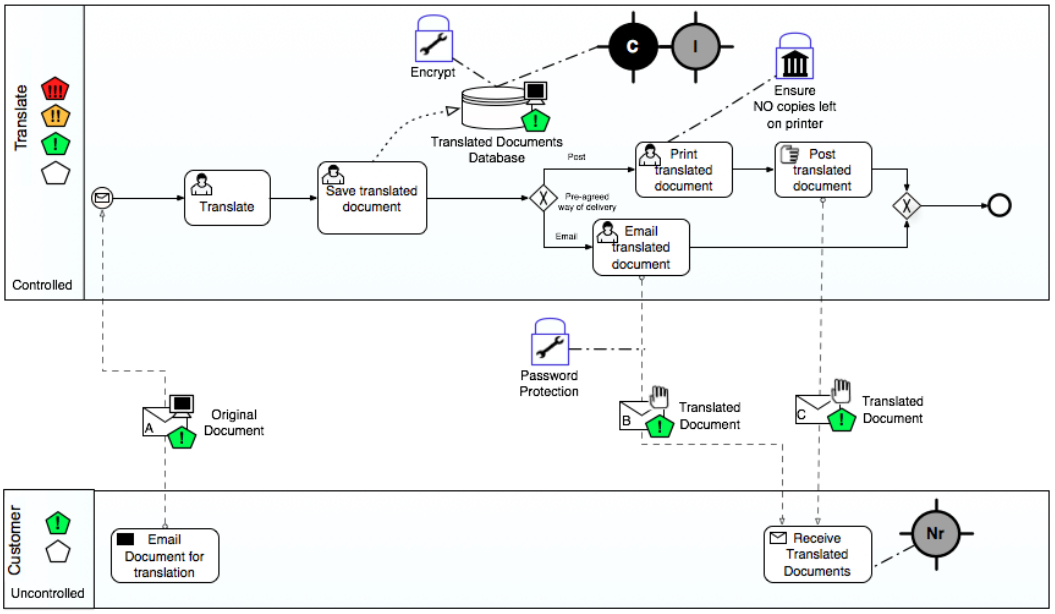


Figure 6: The security-annotated diagram of the translation service provision process.

Q4. A customer sends to Translate an electronic copy of the original document and this document is classified as "Confidential" by Translate.

- Correct
- Partially correct. The document is electronic, but classified as "Proprietary".
- Incorrect
- Not sure

Q5. According to the annotated diagram, Translate may send a document classified as "Proprietary" to a customer.

Correct | Not sure | Incorrect

Q6. The form (format) of one of the messages transmitted between Translate and a customer is marker incorrectly. Please identify which one.

A | B | C | Not sure

Q7. When Translate sends a translated document to a customer by email, a document must be protected with a password.

Correct | Not sure | Incorrect

Q8. * A customer may have access to the financial statements of Translate, which are classified as "Restricted Shearing"?

Correct | Not sure | Incorrect

Q9. A database of translated documents has the same level of sensitivity as an original document received from a customer.

Correct | Not sure | Incorrect

Q10. Translate is concerned with non-repudiation of the receipt of a translated document with medium criticality.

- Correct
- Partially correct. Translate is concerned with non-repudiation, but criticality of this concern is low.
- Incorrect
- Not sure

Q11. With which security goal Translate is concerned with regard to the database of translated documents with high criticality?

- Confidentiality
- Integrity
- Accountability
- Non-repudiation
- Privacy
- Availability
- Authenticity & Trustworthiness
- Auditability
- Not sure

Q12. Why Translate is designated in the diagram as a "controlled" location?

Q13. Please specify which additional (or alternative) security countermeasures may be exploited in the process of the translation service provision. You may choose from a list of suggestions AND/OR name a different countermeasure using the option "Other".

- Organisational Countermeasure: Signed for delivery
- Human-orineted Countermeasure: Training on email encryption
- Technical Countermeasure: Biometrics
- Other, (please specify)

Please explain your choice.

A.19 Interpretation Task (Task 2) Marking Scheme

Table 11: Task 2 Marking Scheme

Variable	Location	Access Permissions	Information Format	Information Sensitivity	Security Goal	Criticality	Security Countermeasure
Question No[a]	Q3+Q12	Q5+Q8	Q4+Q6	Q4 + Q9	Q10 + Q11	Q10 + Q11	Q7+Q13
Allocated Score[b]	Q3 - C - 1	Q5 - C - 1	Q4 - C - 1	Q4 - C - 0	Q10 - C - 1	Q10 - C - 1	Q7 - C - 1
	Q3 - NS - 0	Q5 - NS - 0	Q4 - Partially C - 1	Q4 - PC - 1	Q10 - PC - 0	Q10 - PC - 0	Q7 - NS - 0
	Q3 - InC - 0	Q5 - InC - 0	Q4-InC - 0	Q4-InC - 0	Q10 - InC - 0	Q10 - InC - 0	Q7 - InC - 0
	Q12 - check answer 1/0	Q8 - C - 0	Q4 - NS - 0	Q4 - NS - 0	Q10 - NS - 0	Q10 - NS - 0	Q13 - Signed For - 1
		Q8 - NS - 0	Q6 - A - 0	Q9 - C - 1	Q11 - Confidentiality - 1	Q11 - Confidentiality - 1	Q13 - Training - 0
		Q8 - I - 1	Q6 - B - 1	Q9 - NS - 0	Q11 - other goal - 0	Q11 - other goal - 0	Q13 - Biometrics - 0
			Q6 - C - 0	Q9 - I - 0			Q13 - check answer 1/0

[a]Number of the question as it appeared in Task 2 (Appendix A.18).

[b]C - Correct; PC -Partially Correct; I - Incorrect; NS - Not sure

A.20 Secure*BPMN Evaluation. Post-task Survey

Note: for traceability and consistency the numbering of questions is maintained as it appeared in the actual survey. Questions 3-13 in the actual questionnaire related to the performance of the interpretation task (Task 2) and are presented in Appendix A.18.

Part 1. Demographic Data.

Q15. Your country

Q16. Your role in an organisation

Q17. Your level of expertise in business processes

No knowledge | Some knowledge | Quite knowledgeable | Expert

Q18. Your level of expertise in BPMN, specifically

No knowledge | Some knowledge | Quite knowledgeable | Expert

Q19. For what purpose do you model business processes?

Q20. How many years of experience do you have working with BPMN?

Q21. Your level of expertise in Information Assurance and/or Information Security

No knowledge | Some knowledge | Quite knowledgeable | Expert

Q22. How many years of experience do you have in Information Assurance and Security?

Q23. If you have expertise in Information Assurance and/or Information Security, please specify what is your particular area of specialisation in this domain?

Part 2. Performance Metrics.

Q44. How many MINUTES did it take you to perform the annotation task (TASK1)?

Q14. How many MINUTES did the task take?

Part 3. Evaluation of Secure*BPMN according to the Method Evaluation Model.

Q24. Secure*BPMN is useful for the security annotation of business process models.

Strongly Disagree | Disagree | Agree | Strongly Agree

Q25. Secure*BPMN would facilitate communication with regard to security in business processes.

Strongly Disagree | Disagree | Agree | Strongly Agree

Q26. Learning Secure*BPMN is easy.

Strongly Disagree | Disagree | Agree | Strongly Agree

Q27. I am now competent to apply Secure*BPMN in practice.

Strongly Disagree | Disagree | Agree | Strongly Agree

Q28. In the future, if I will require to security annotate business process models, my intention would be to use Secure*BPMN.

Strongly Disagree | Disagree | Agree | Strongly Agree

Q29. I prefer to continue to use Secure*BPMN for security annotation over other security extensions.

Strongly Disagree | Disagree | Agree | Strongly Agree

Q30. Using Secure*BPMN for security annotation of process models is easy.

Strongly Disagree | Disagree | Agree | Strongly Agree

Q31. In the future, if I will require to gain a comprehensive vision of security issues in a business process, my intention would be to use Secure*BPMN.

Strongly Disagree | Disagree | Agree | Strongly Agree

Q32. Secure*BPMN provides syntax for modelling of ALL security concepts I require to visualise in business process models.

Strongly Disagree | Disagree | Agree | Strongly Agree

Q33. The Secure*BPMN syntax (symbols, icons and applications rules) is intuitive, clear and easy to grasp.

Strongly Disagree | Disagree | Agree | Strongly Agree

Q34. Secure*BPMN would make security concerns in business process models easy to see and understand.

Strongly Disagree | Disagree | Agree | Strongly Agree

Q35. Secure*BPMN provides an effective solution for representing security concerns in business process models.

Strongly Disagree | Disagree | Agree | Strongly Agree

A.21 Secure*BPMN Evaluation. Task 1 - Annotated Diagrams

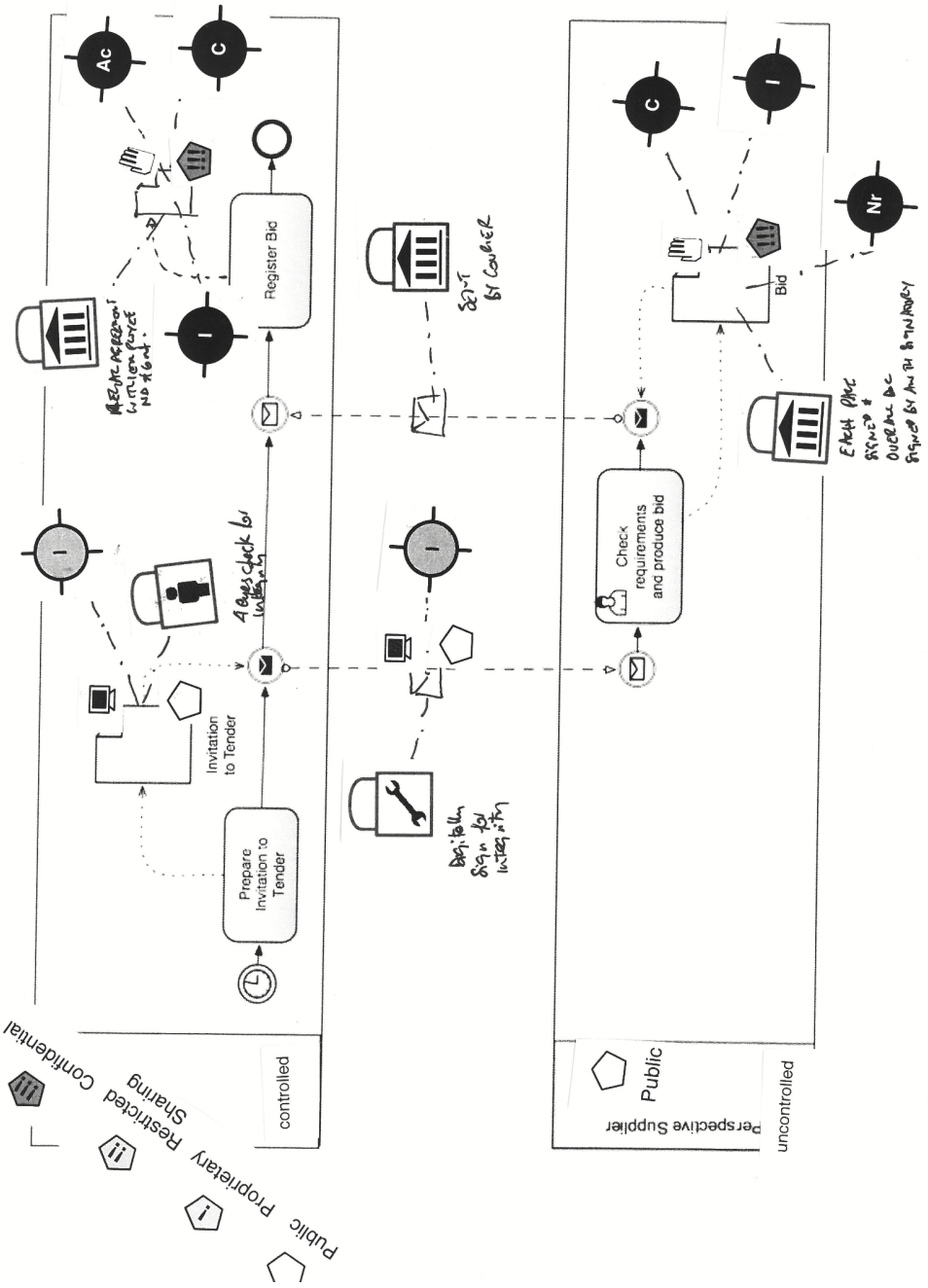


Figure 7: Task 1. Participant 1.

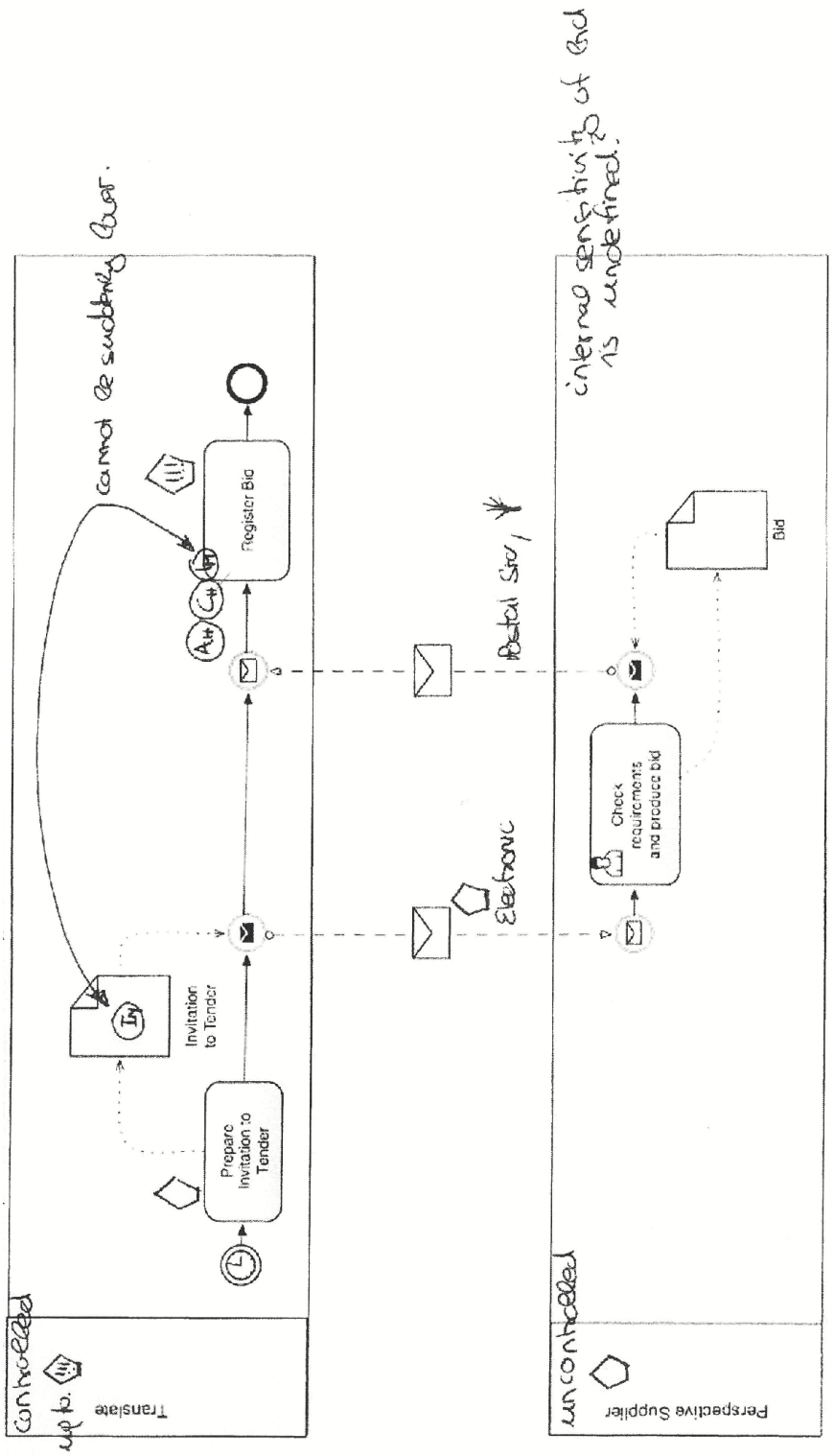


Figure 8: Task 1. Participant 2.

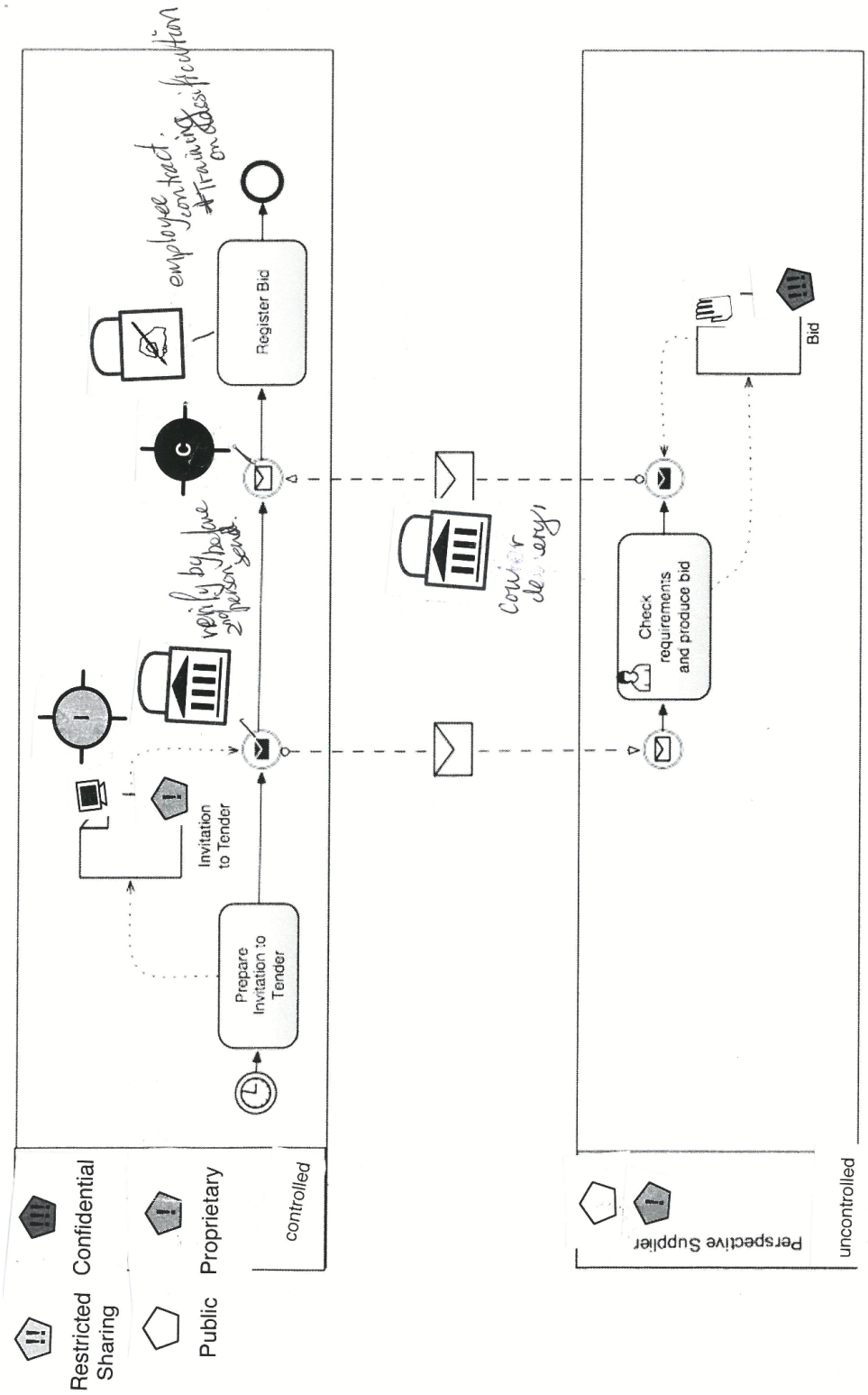


Figure 9: Task 1. Participant 3.

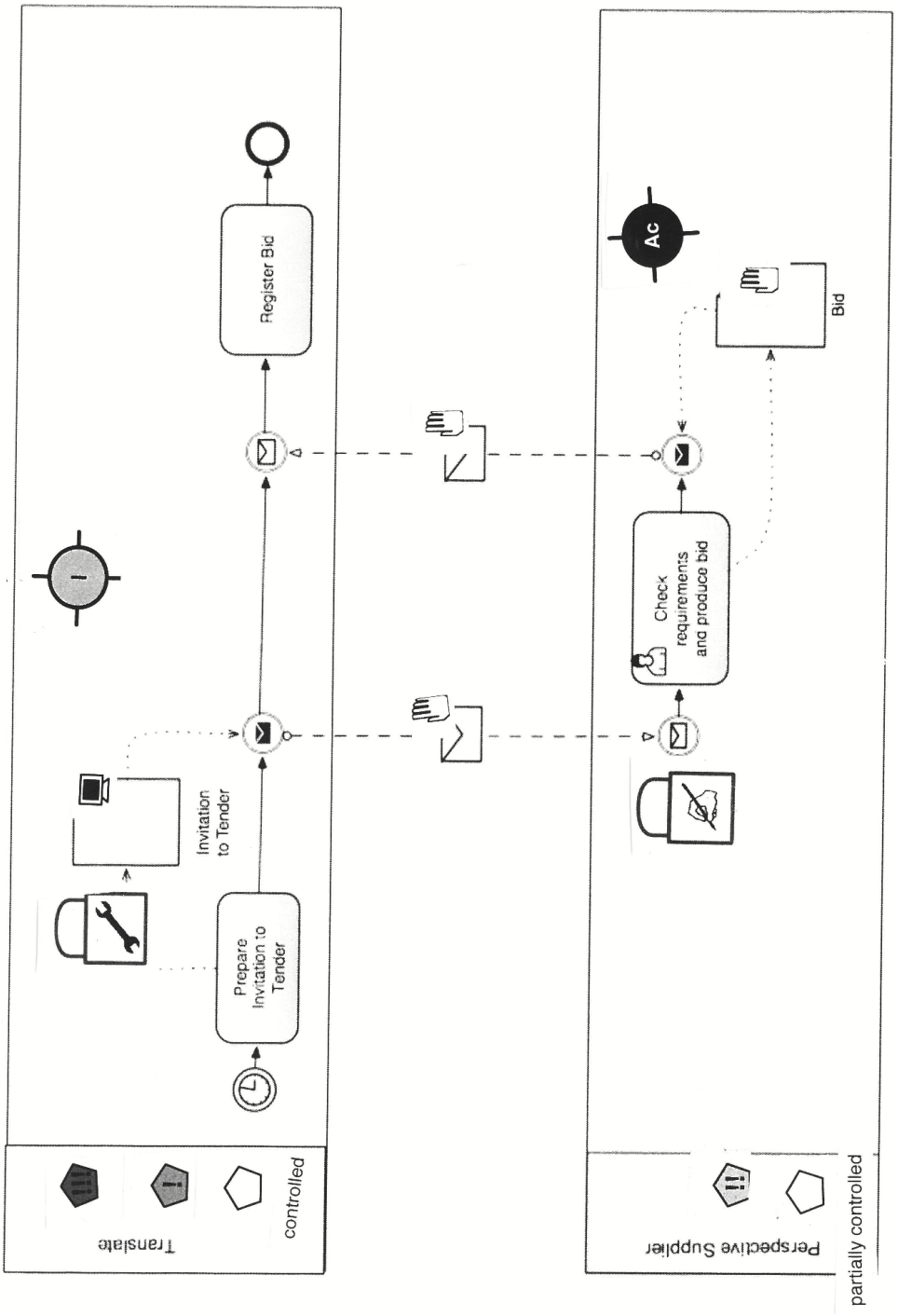


Figure 10: Task 1. Participant 4.

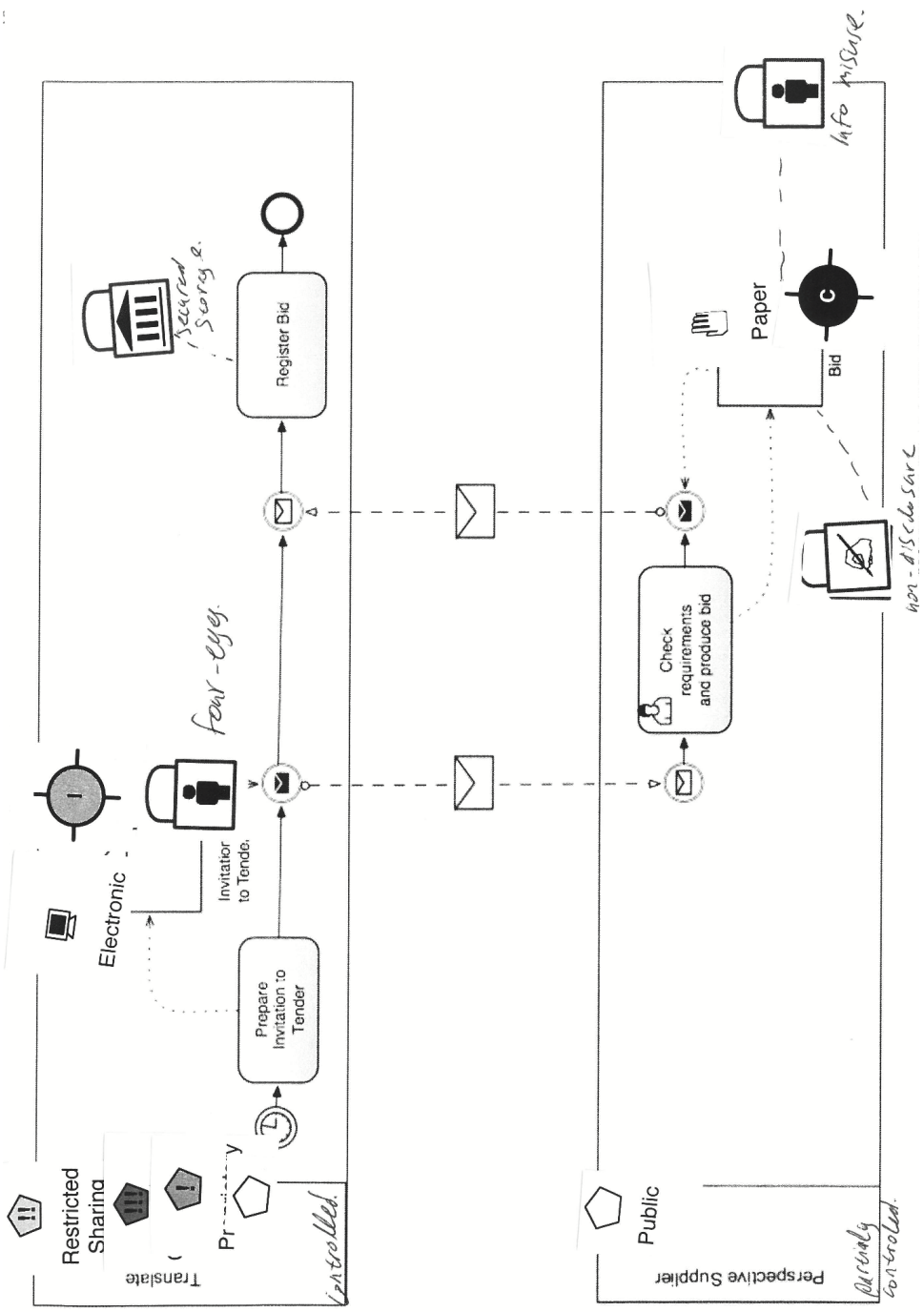


Figure 11: Task 1. Participant 5.

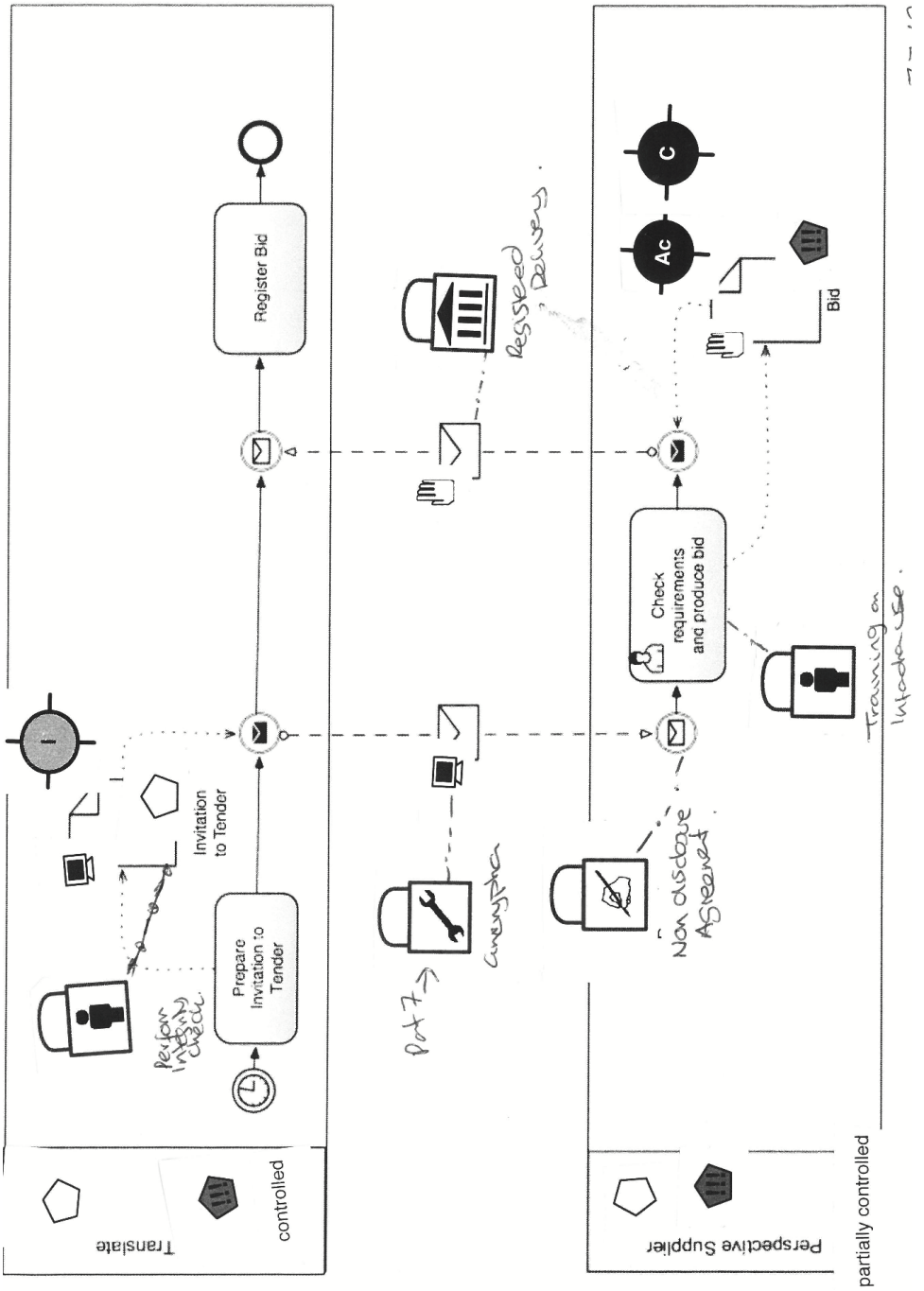


Figure 12: Task 1. Participant 6.

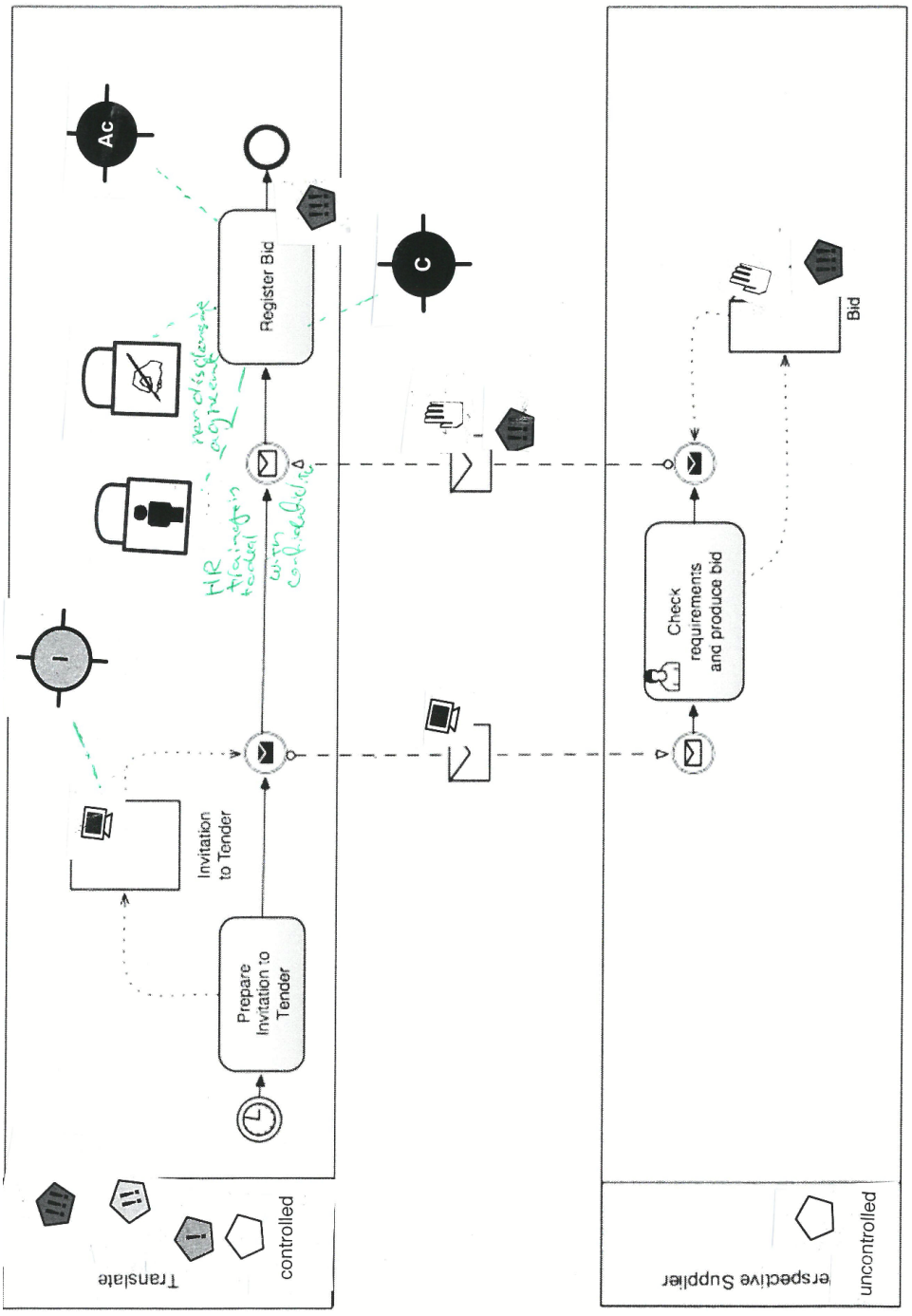


Figure 13: Task 1. Participant 7.

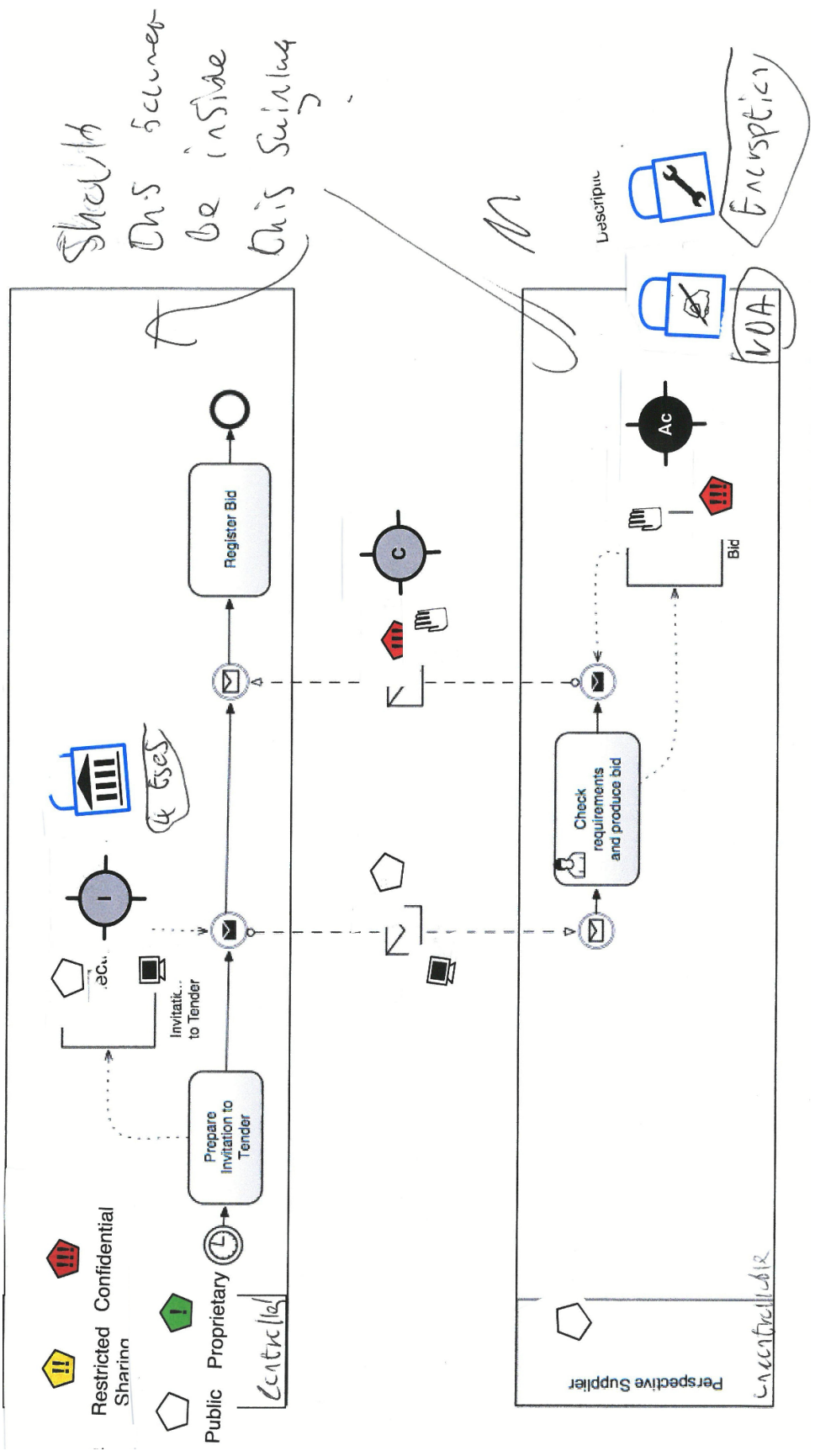


Figure 14: Task 1. Participant 8.

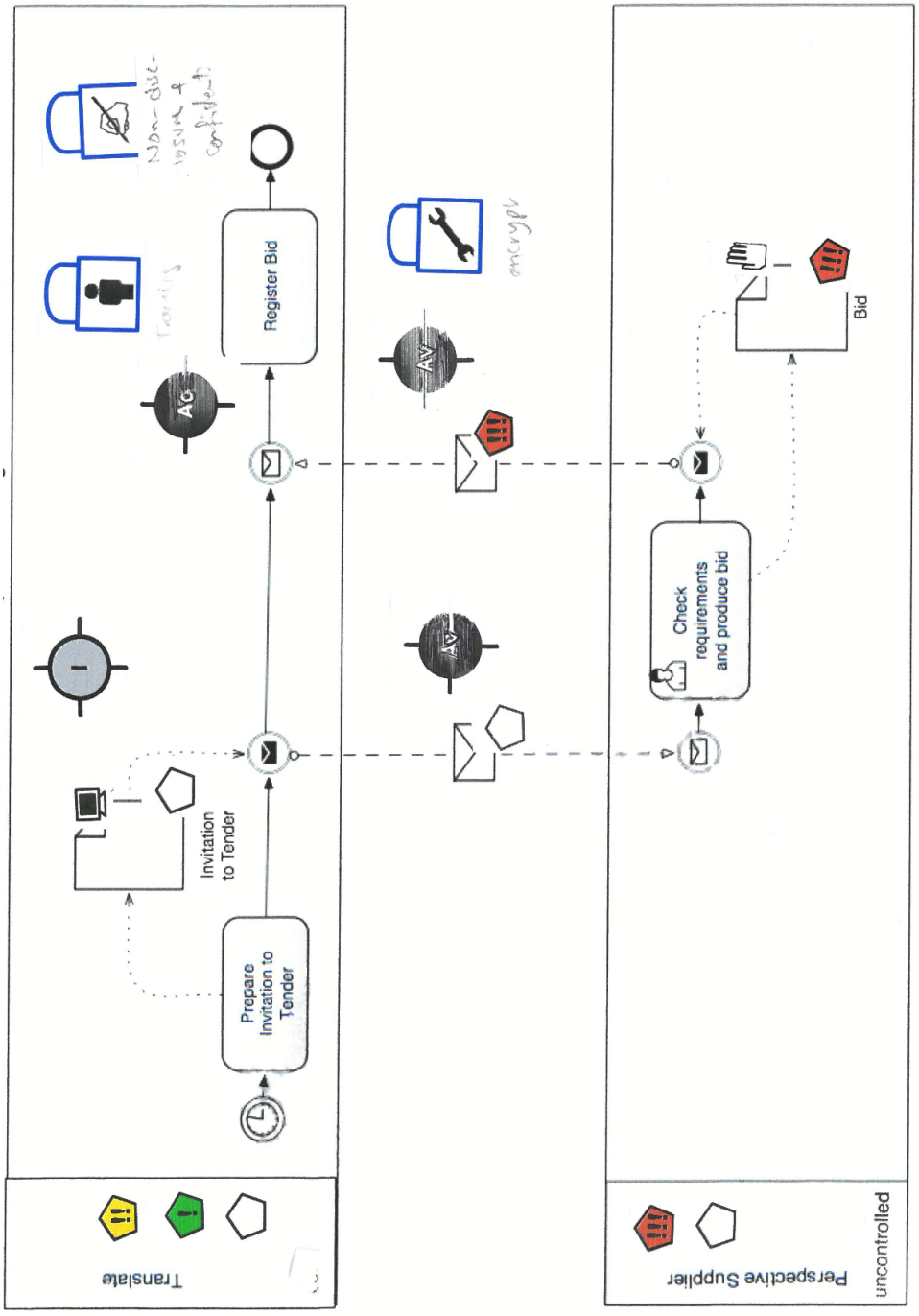


Figure 15: Task 1. Participant 9.

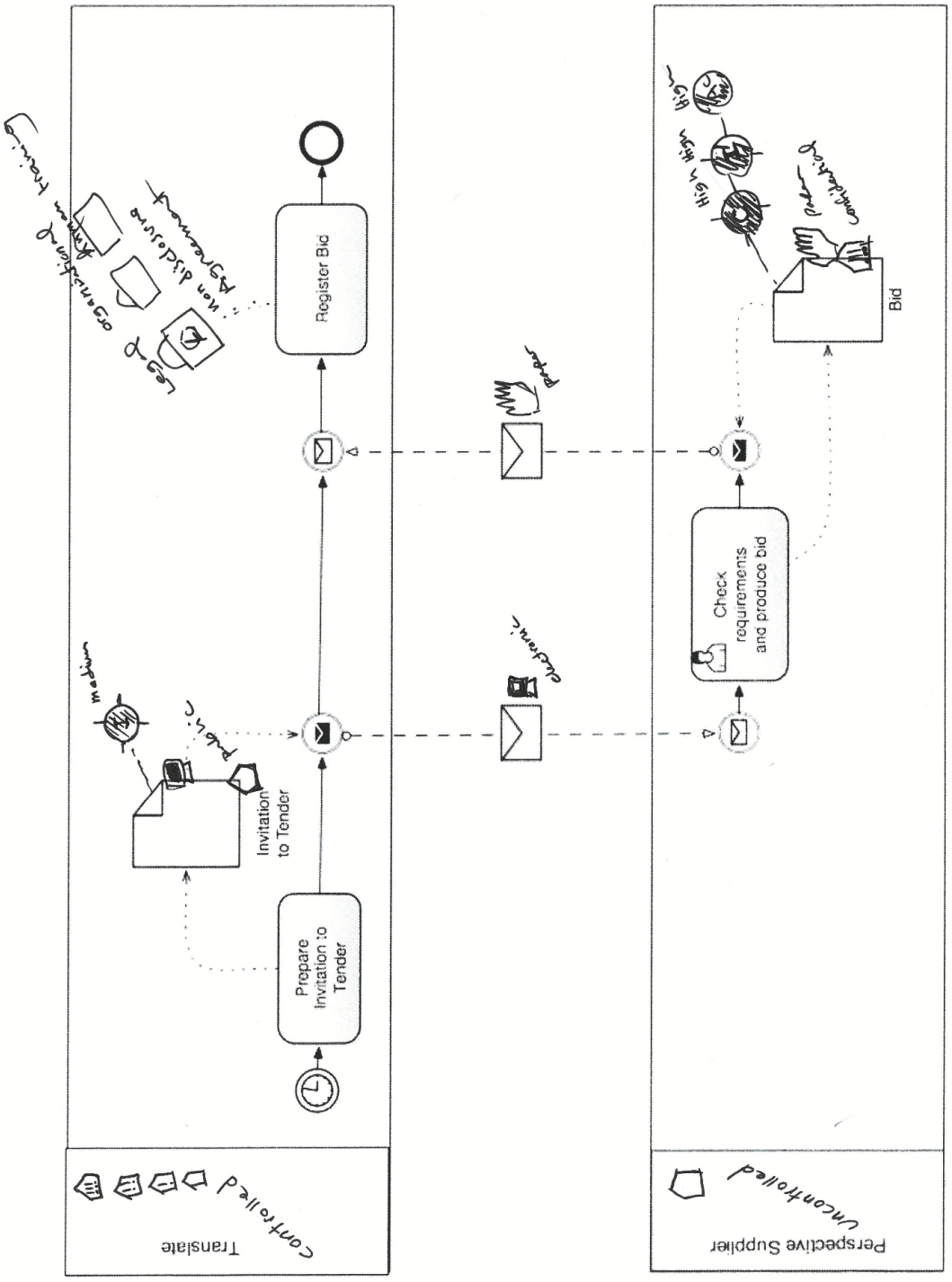


Figure 16: Task 1. Participant 10.

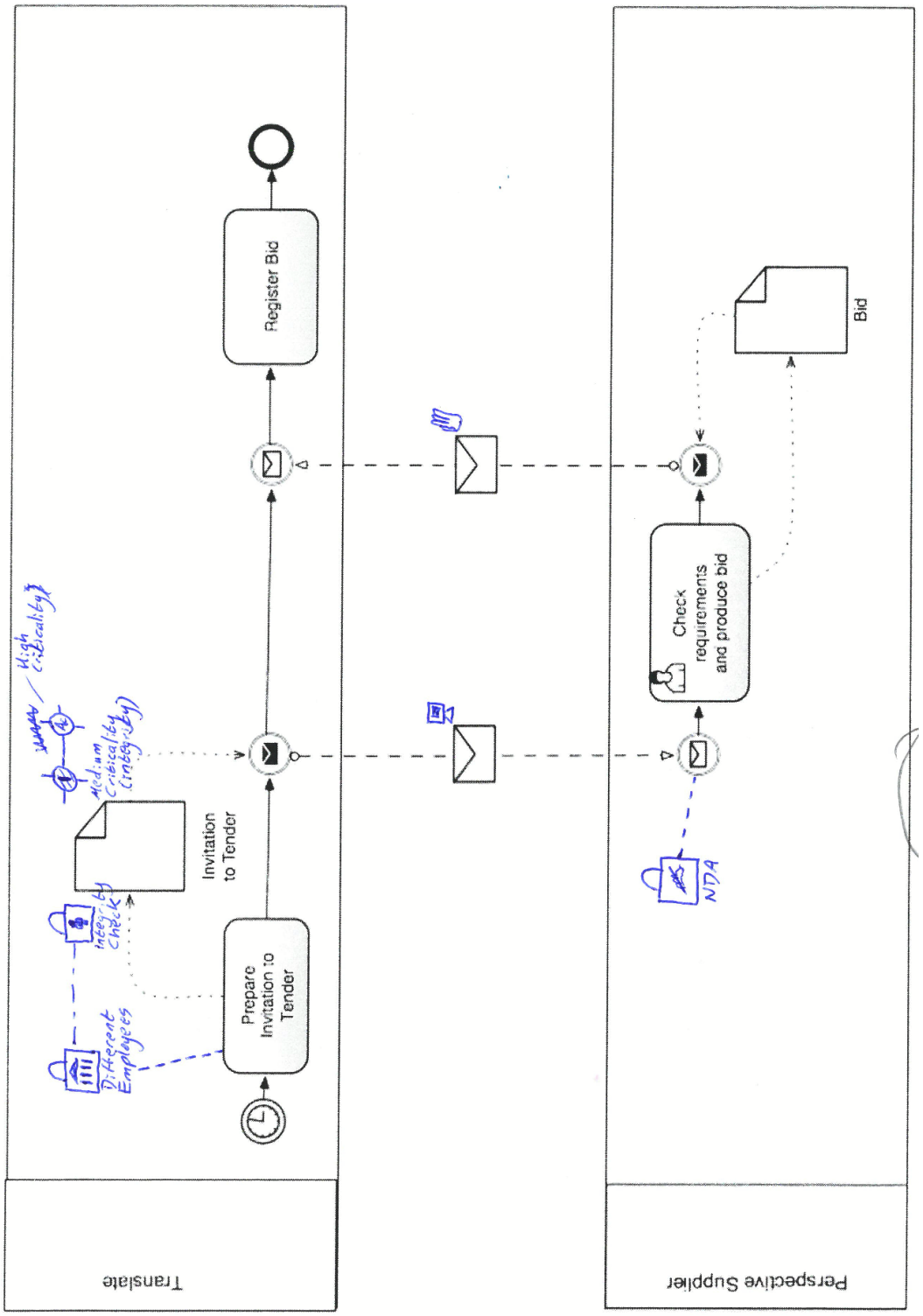


Figure 17: Task 1. Participant 11.

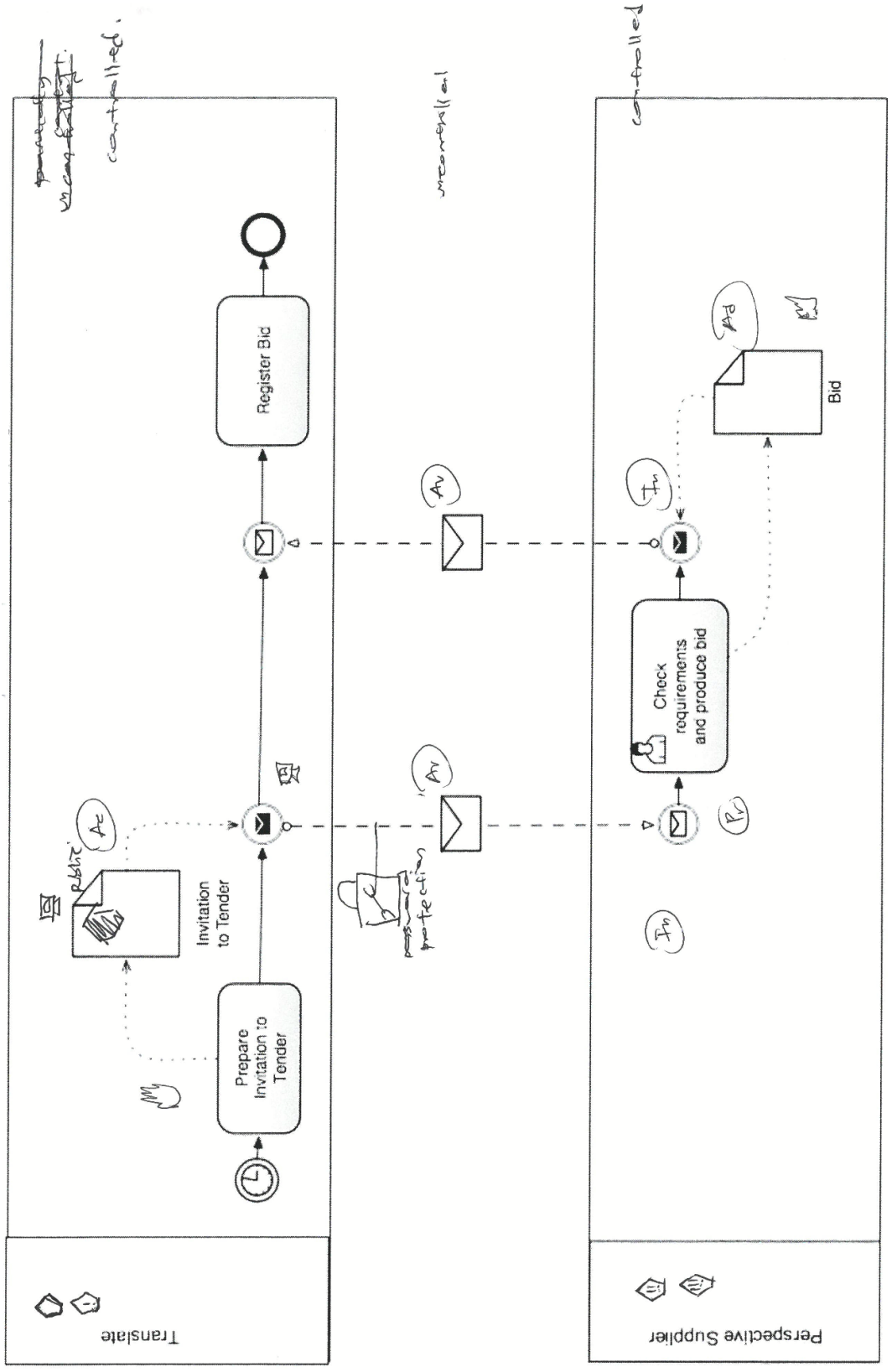


Figure 18: Task 1. Participant 12.

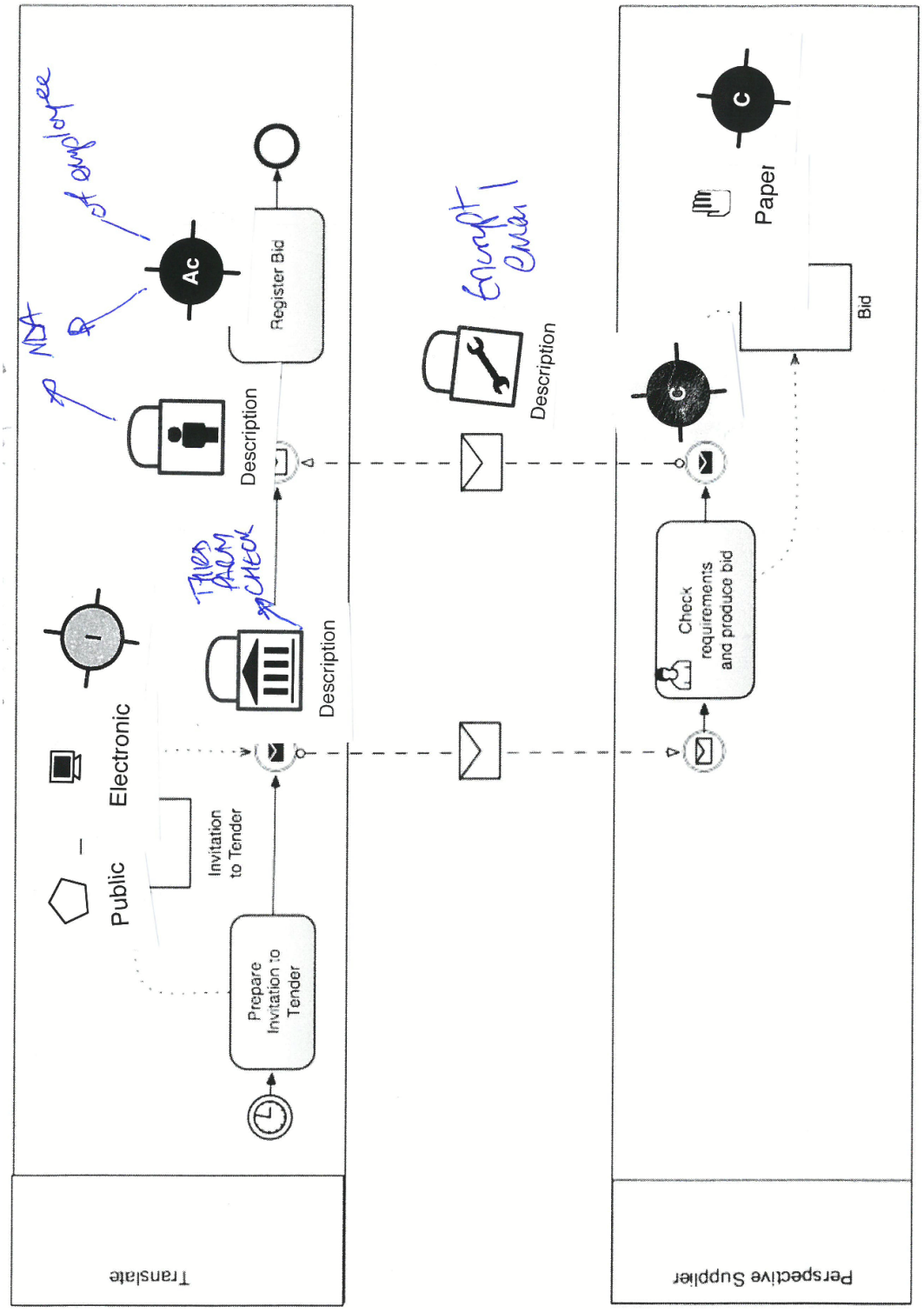


Figure 19: Task 1. Participant 13.

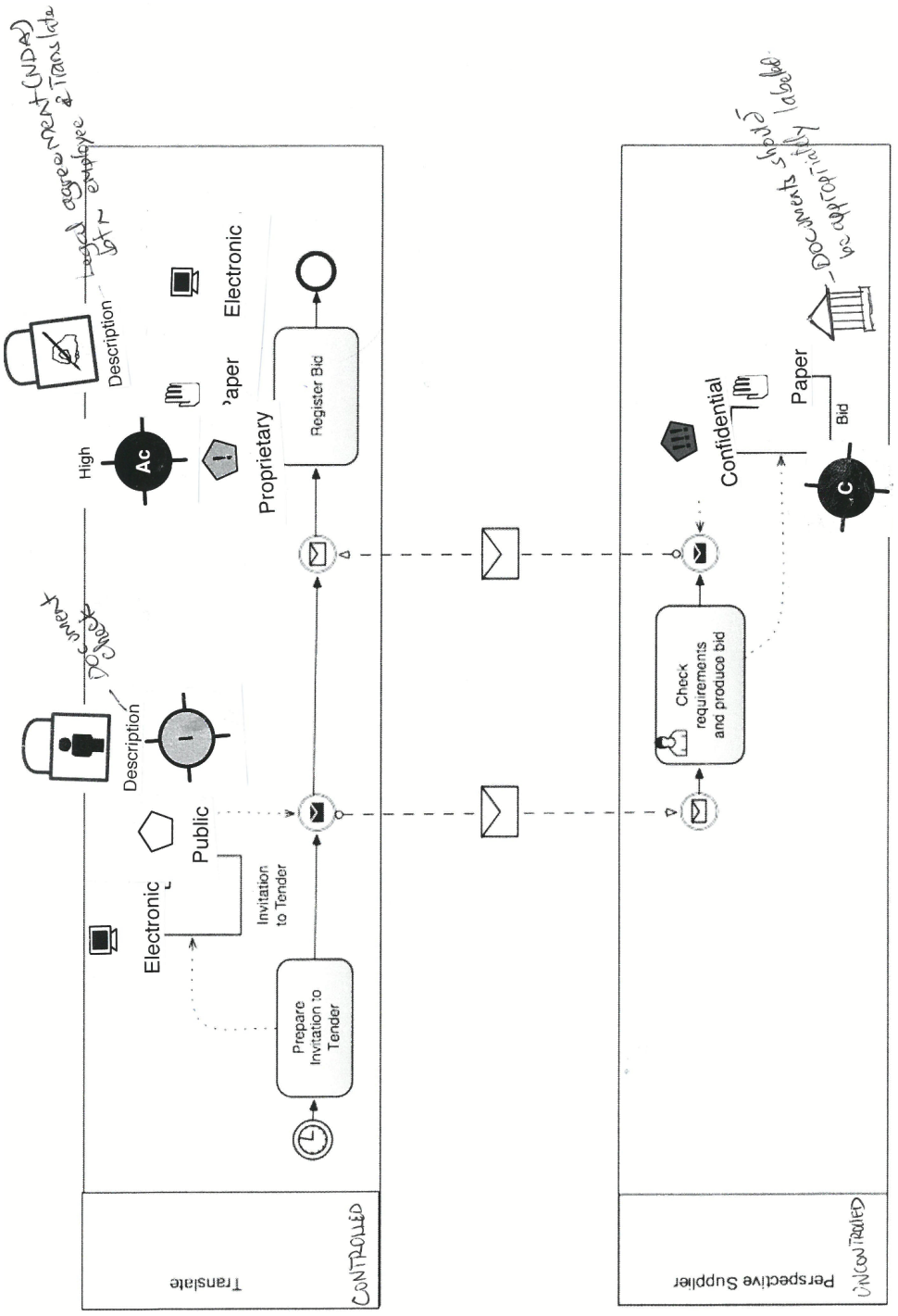


Figure 20: Task 1. Participant 14.

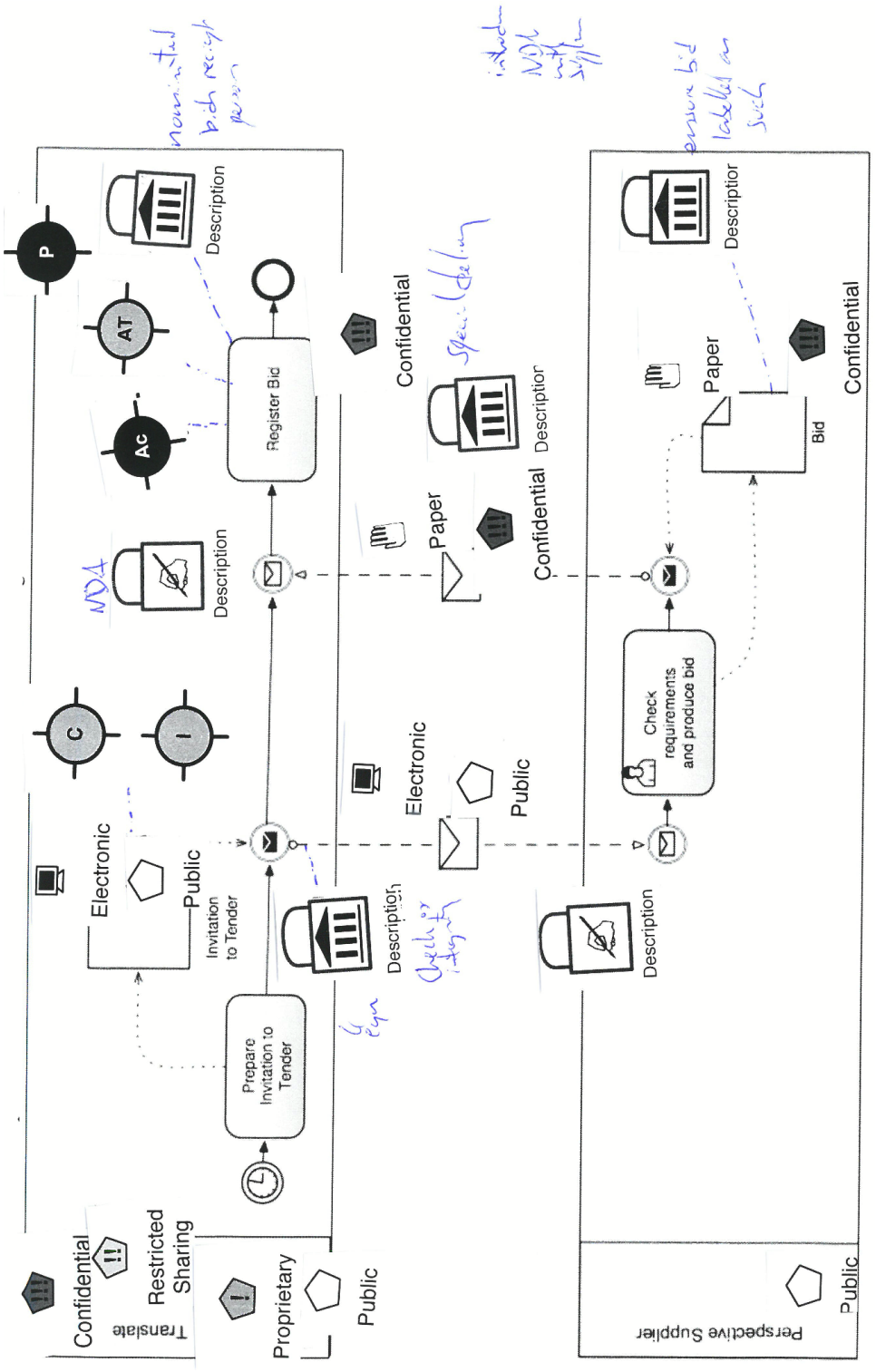


Figure 21: Task 1. Participant 15.

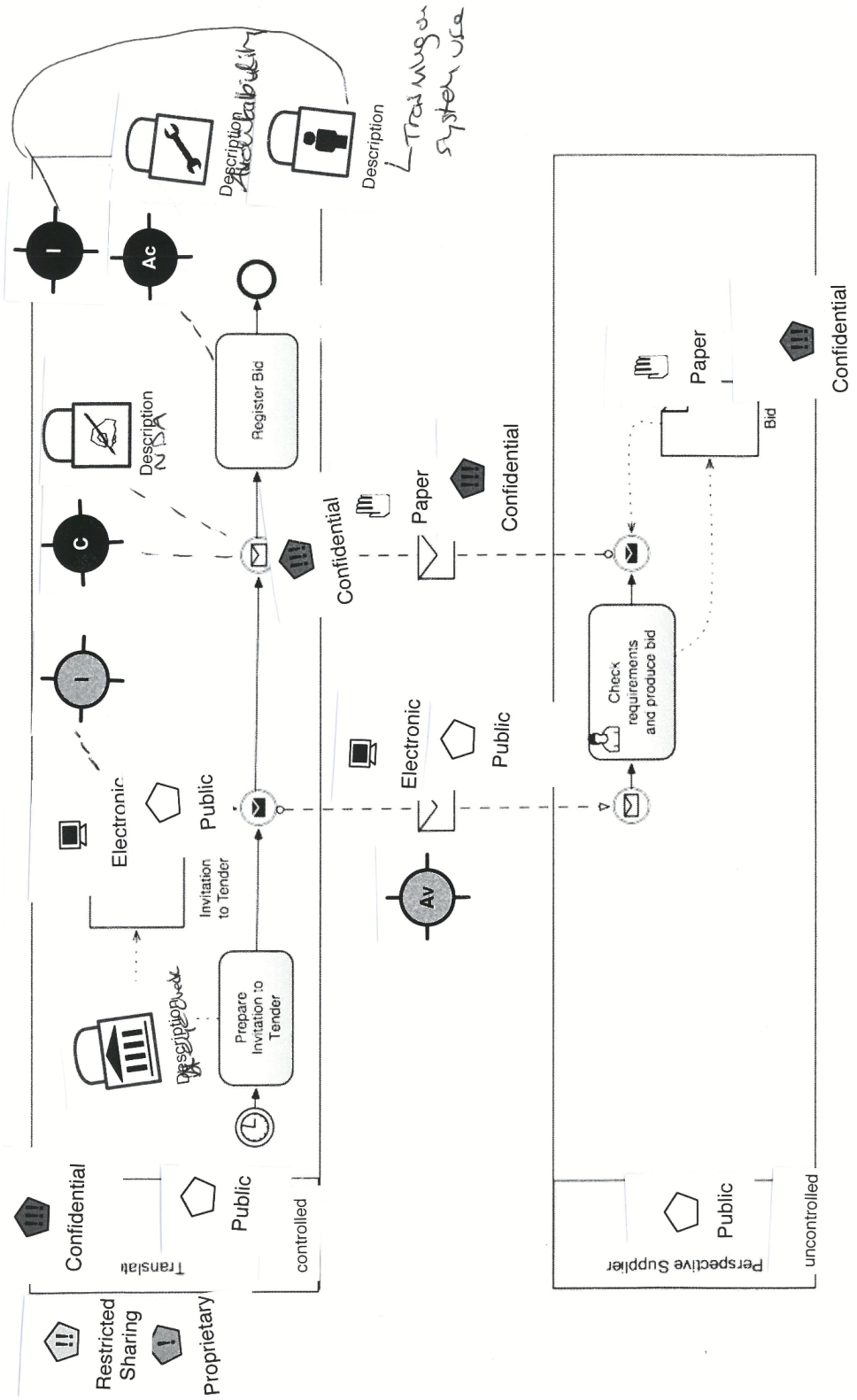


Figure 22: Task 1. Participant 16.

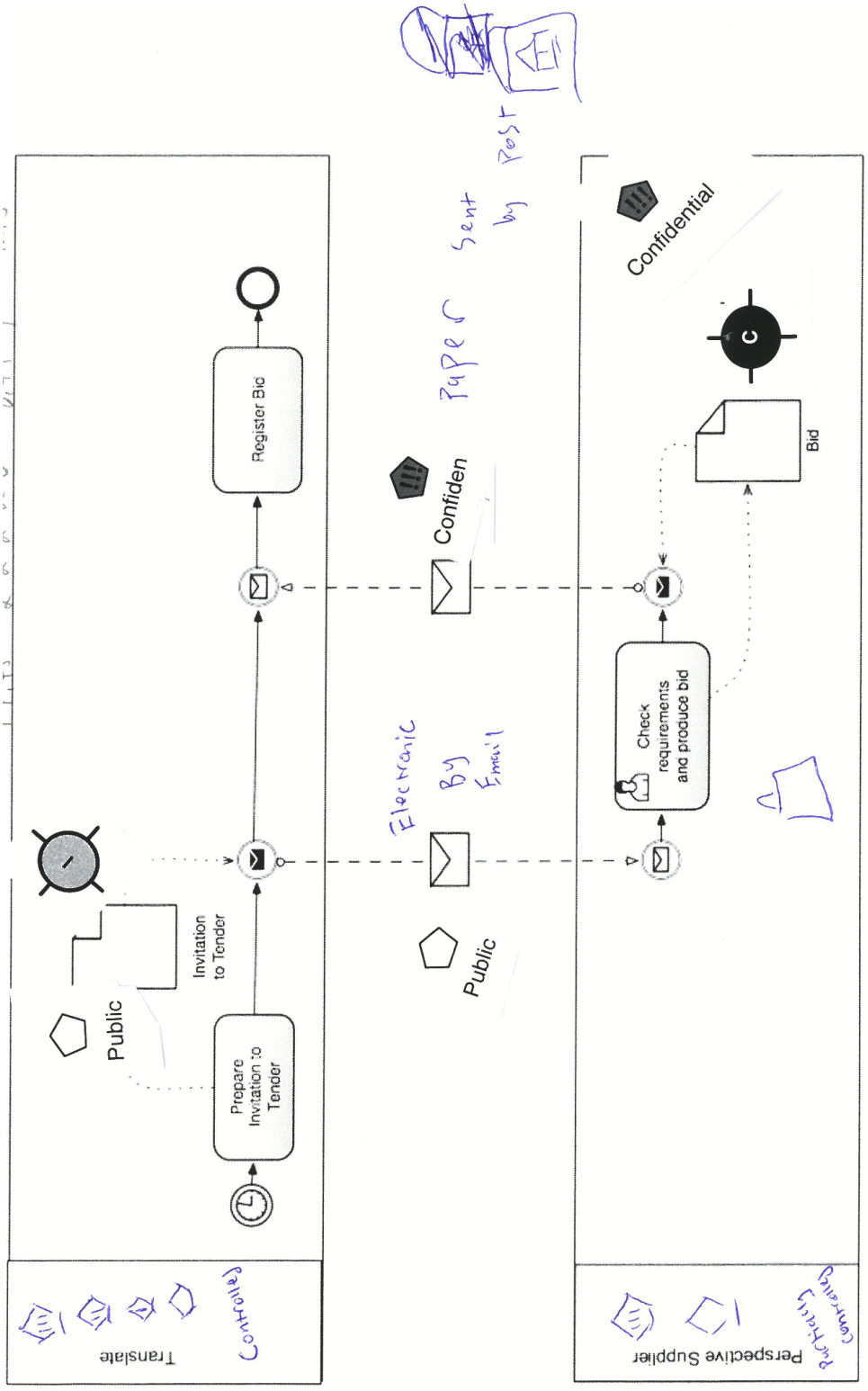


Figure 23: Task 1. Participant 17.

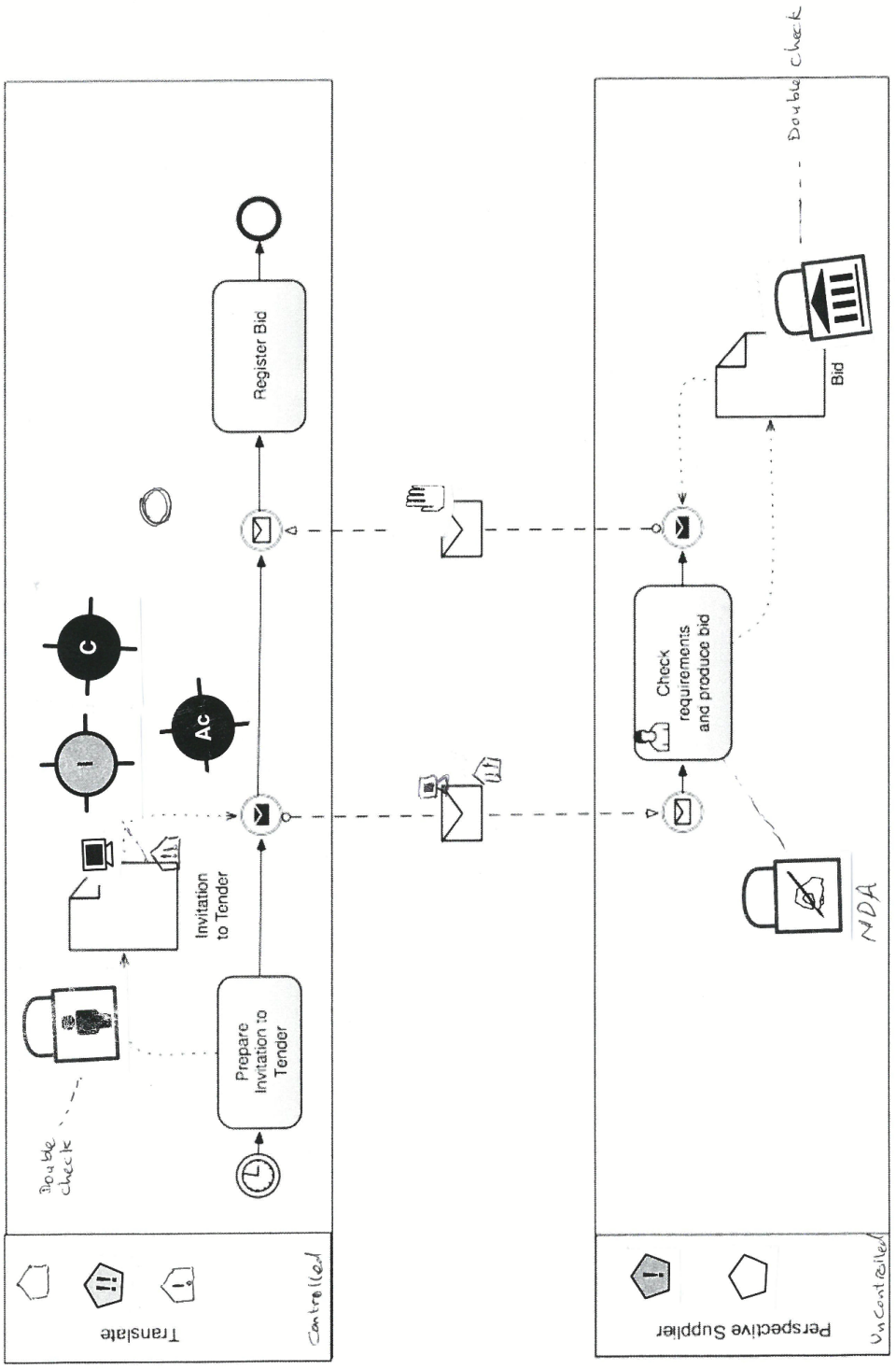


Figure 24: Task 1. Participant 18.

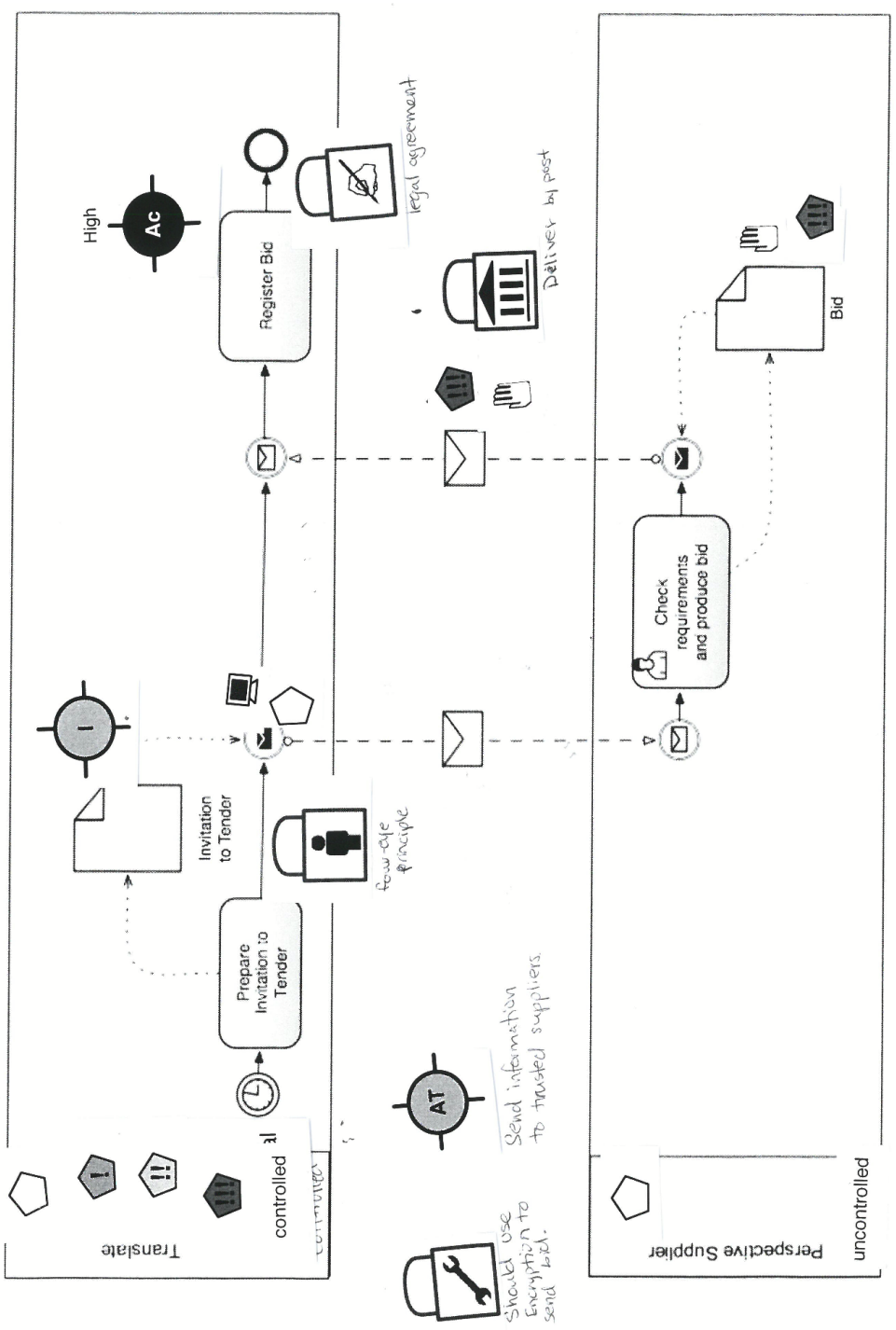


Figure 25: Task 1. Participant 19.

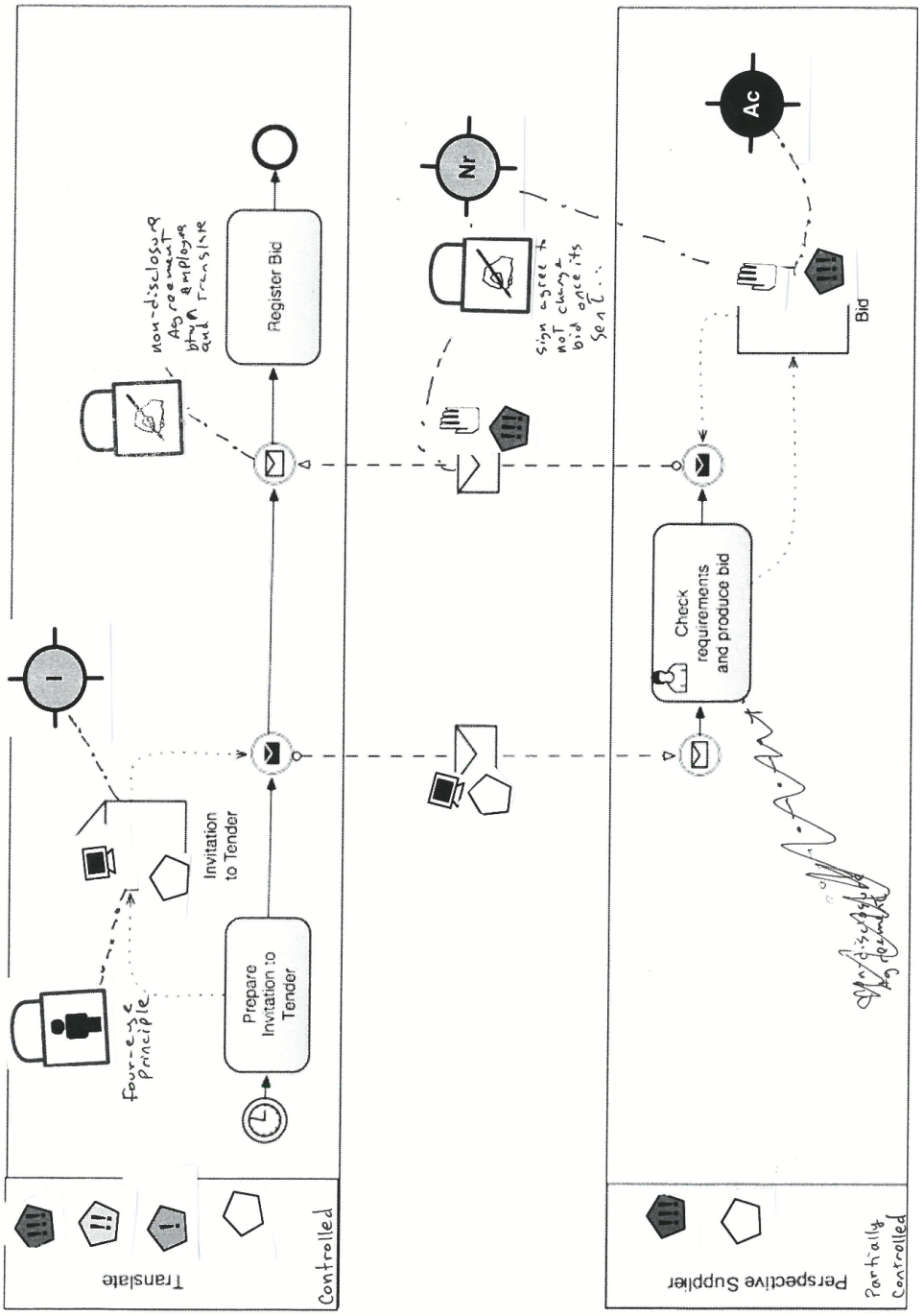


Figure 26: Task 1. Participant 20.

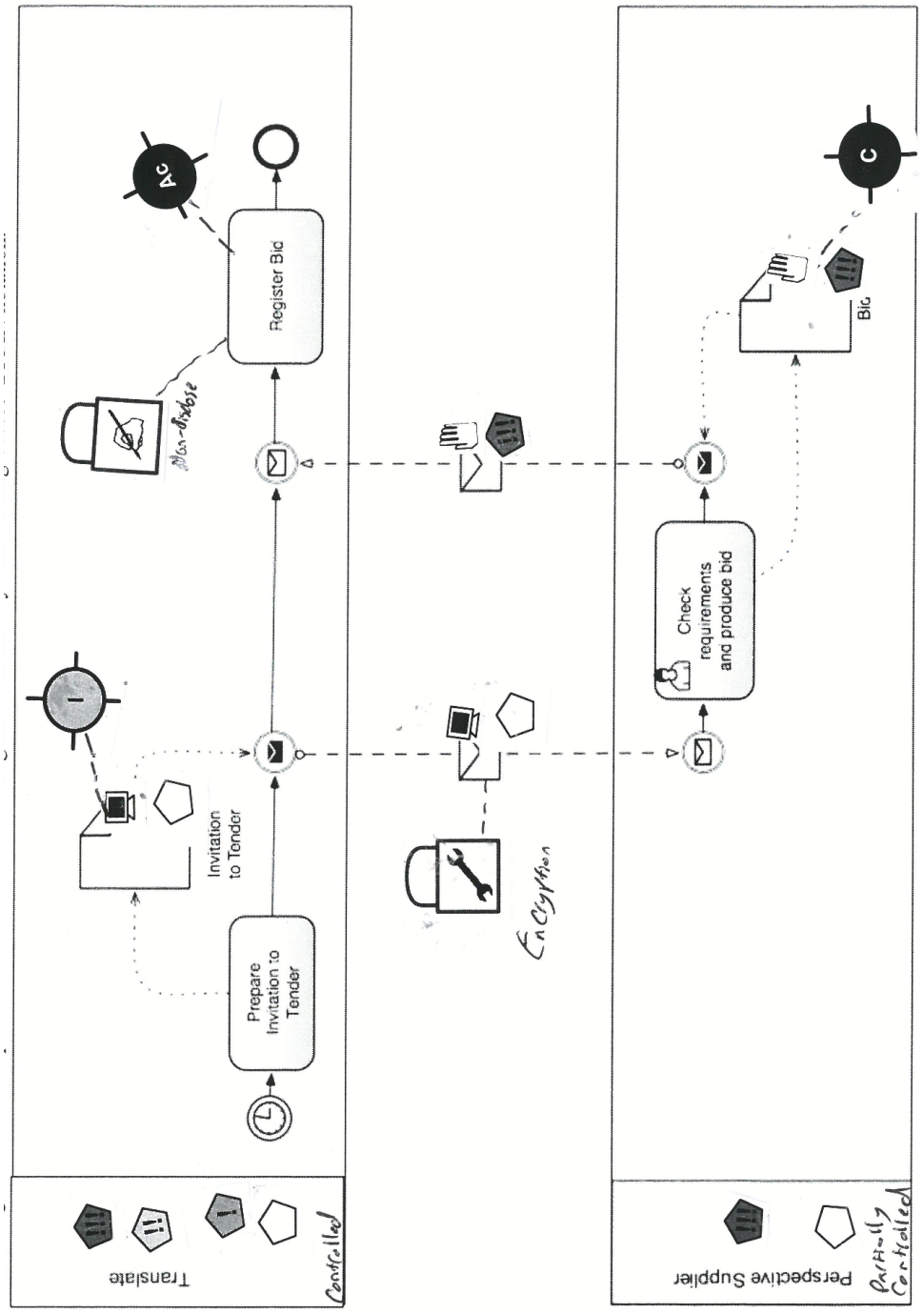


Figure 27: Task 1. Participant 21.

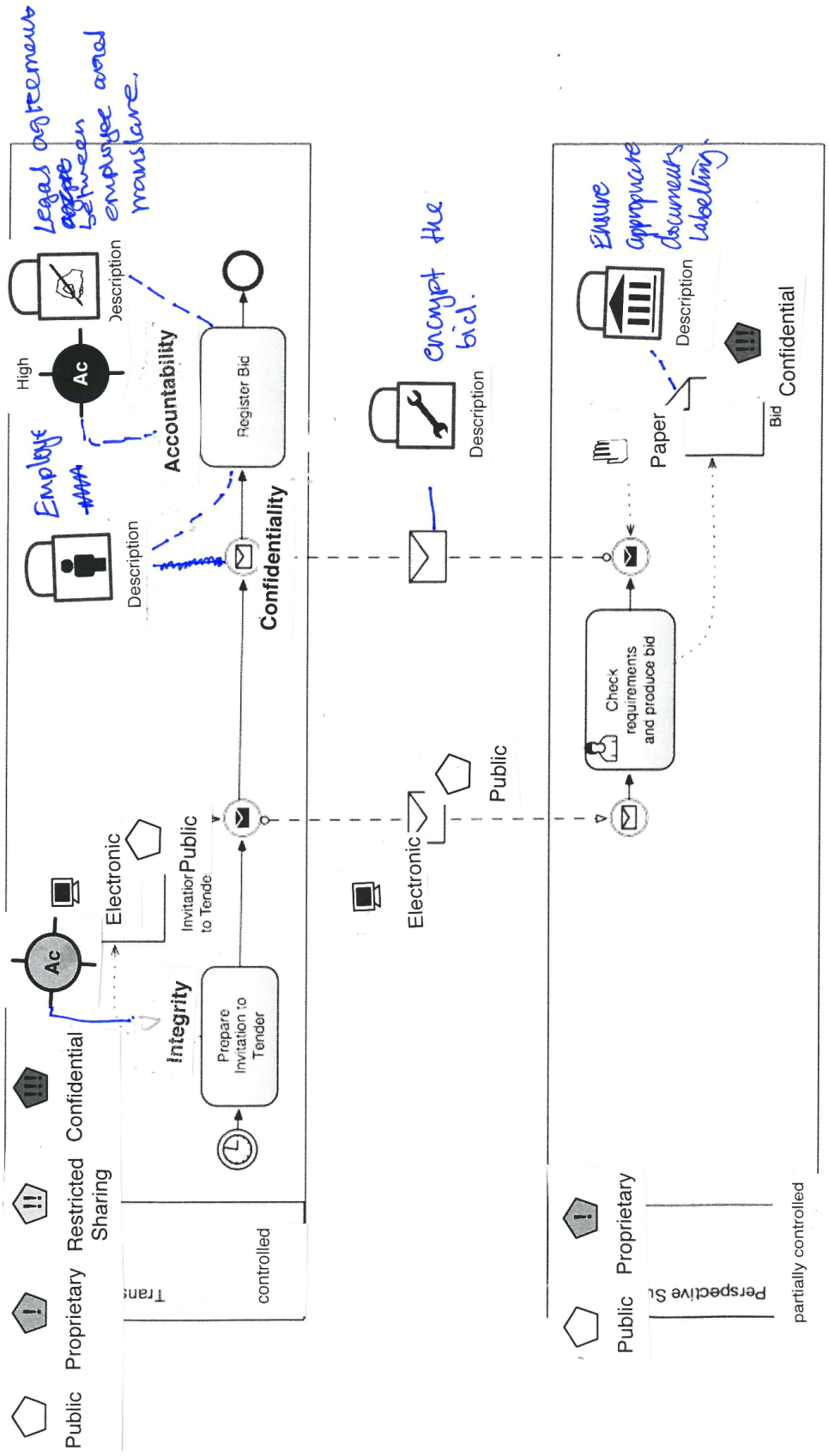


Figure 28: Task 1. Participant 22.

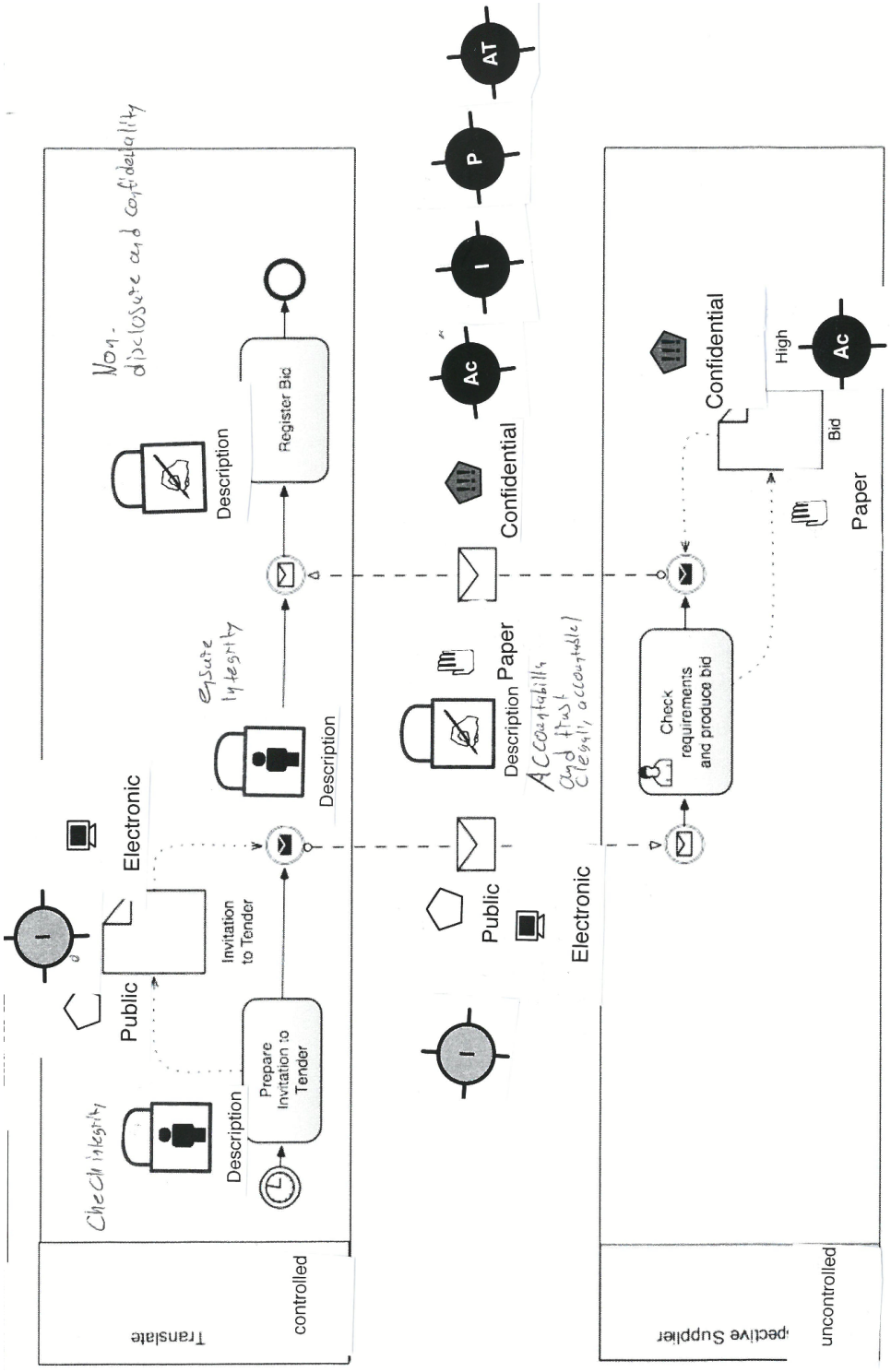


Figure 29: Task 1. Participant 23.

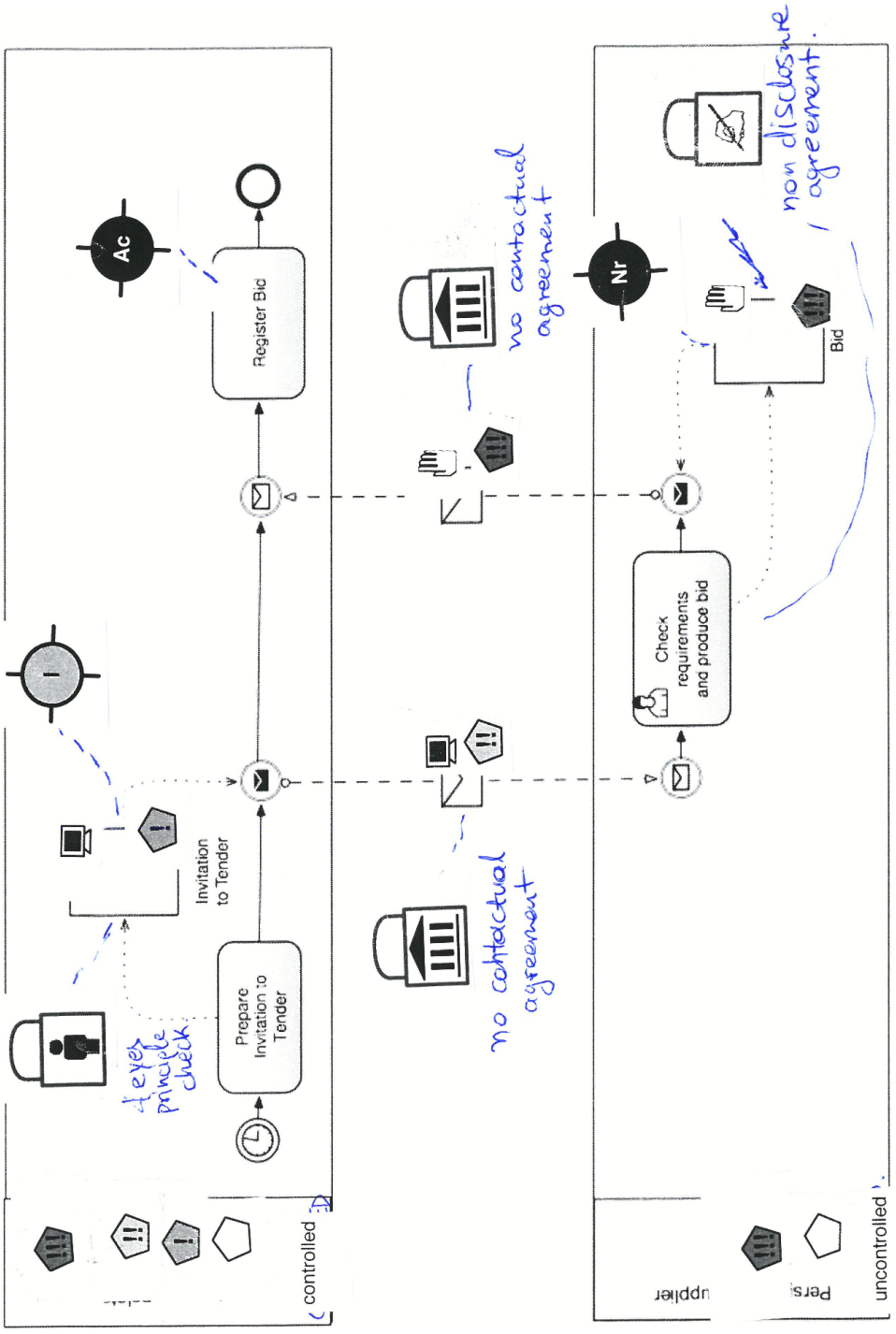


Figure 30: Task 1. Participant 24.

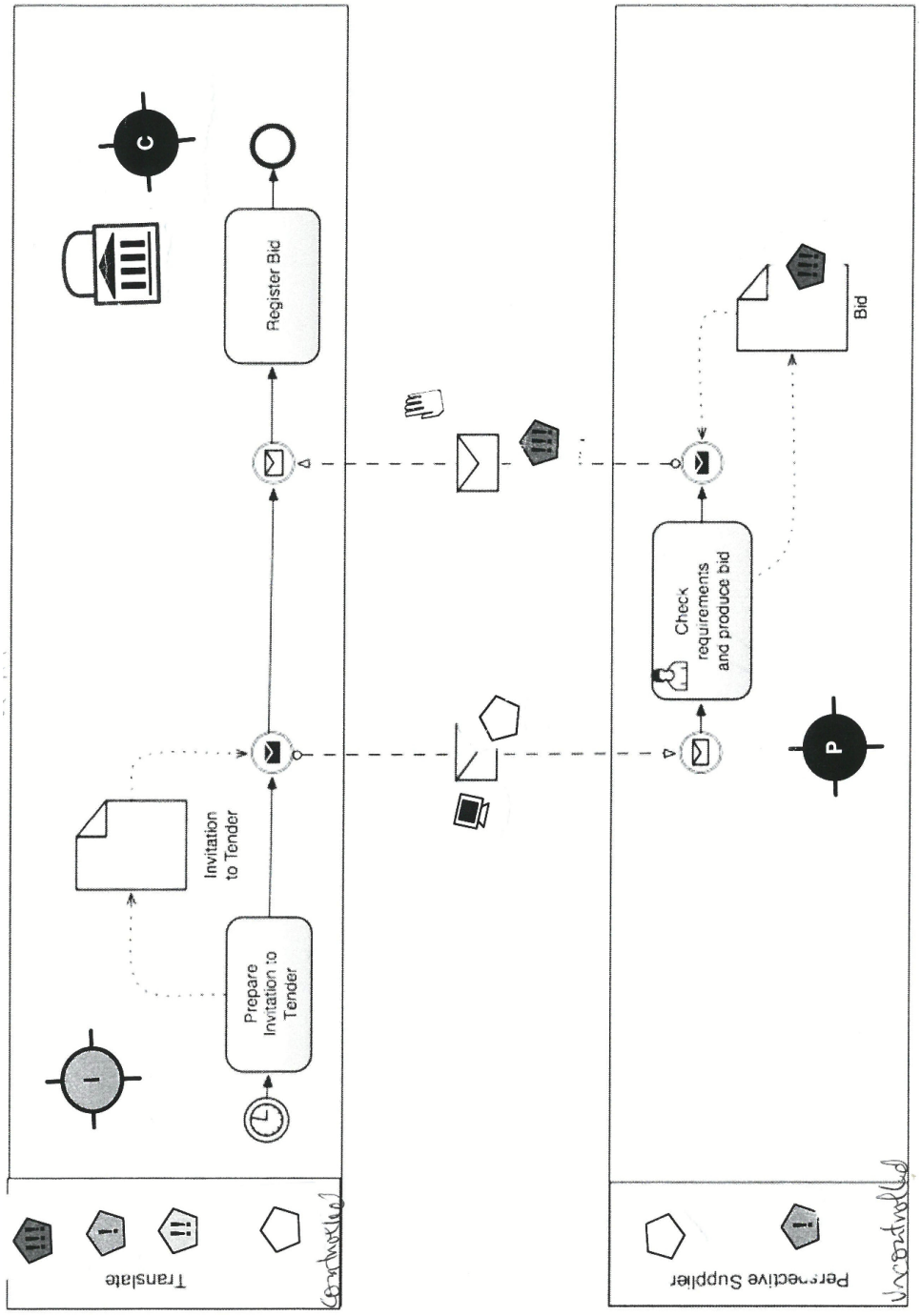


Figure 31: Task 1. Participant 25.

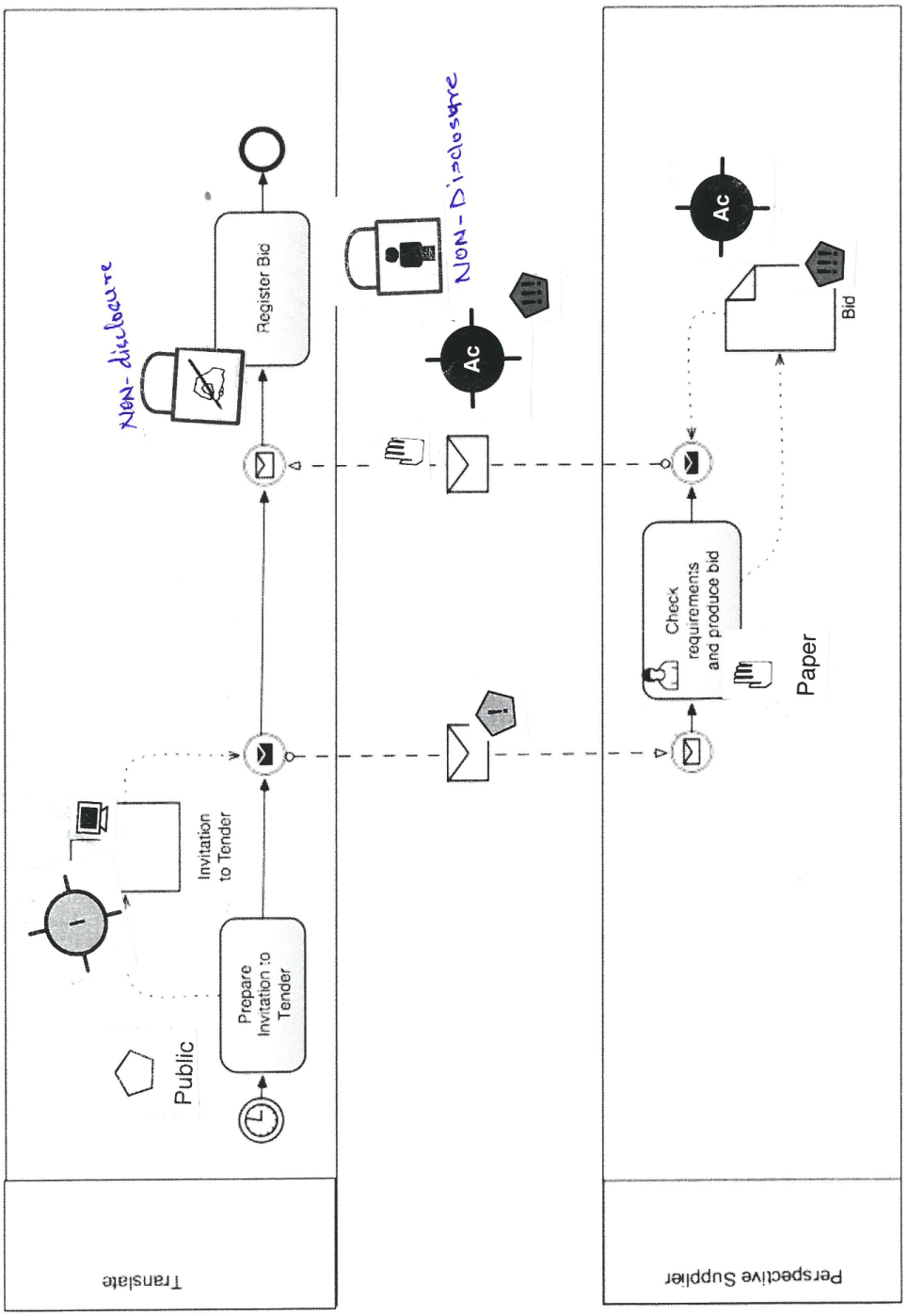


Figure 32: Task 1. Participant 26.

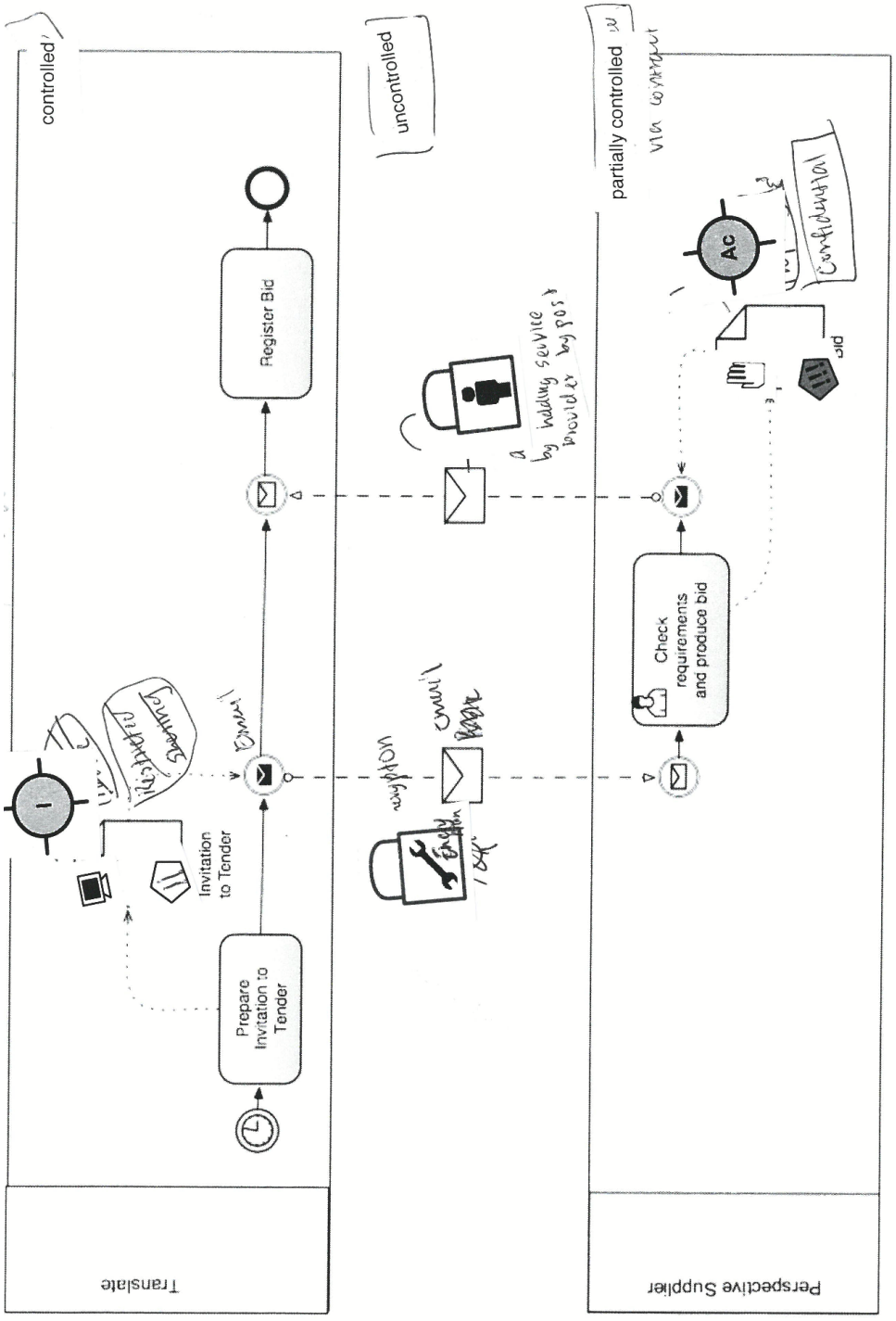


Figure 33: Task 1. Participant 27.

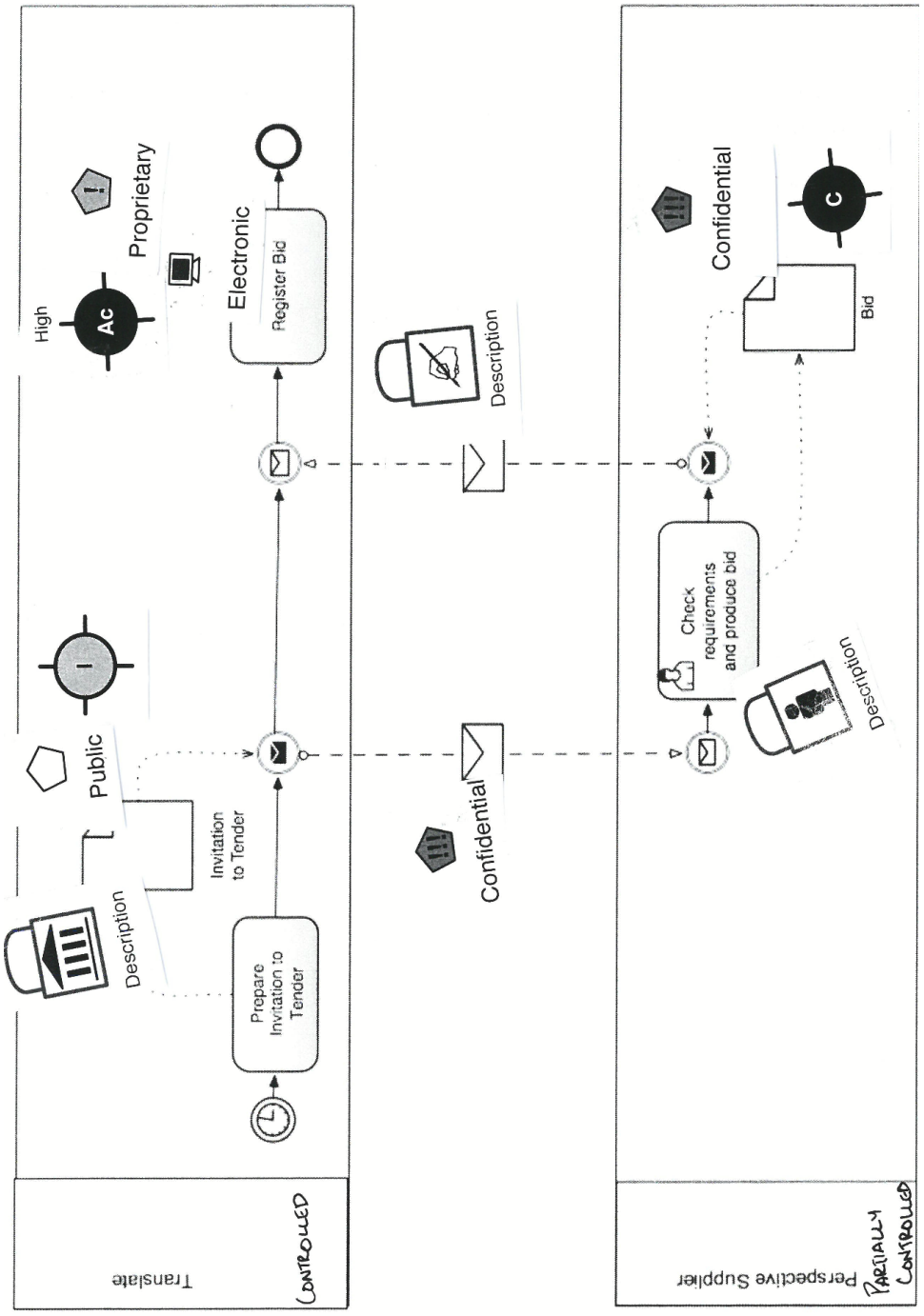


Figure 34: Task 1. Participant 28.

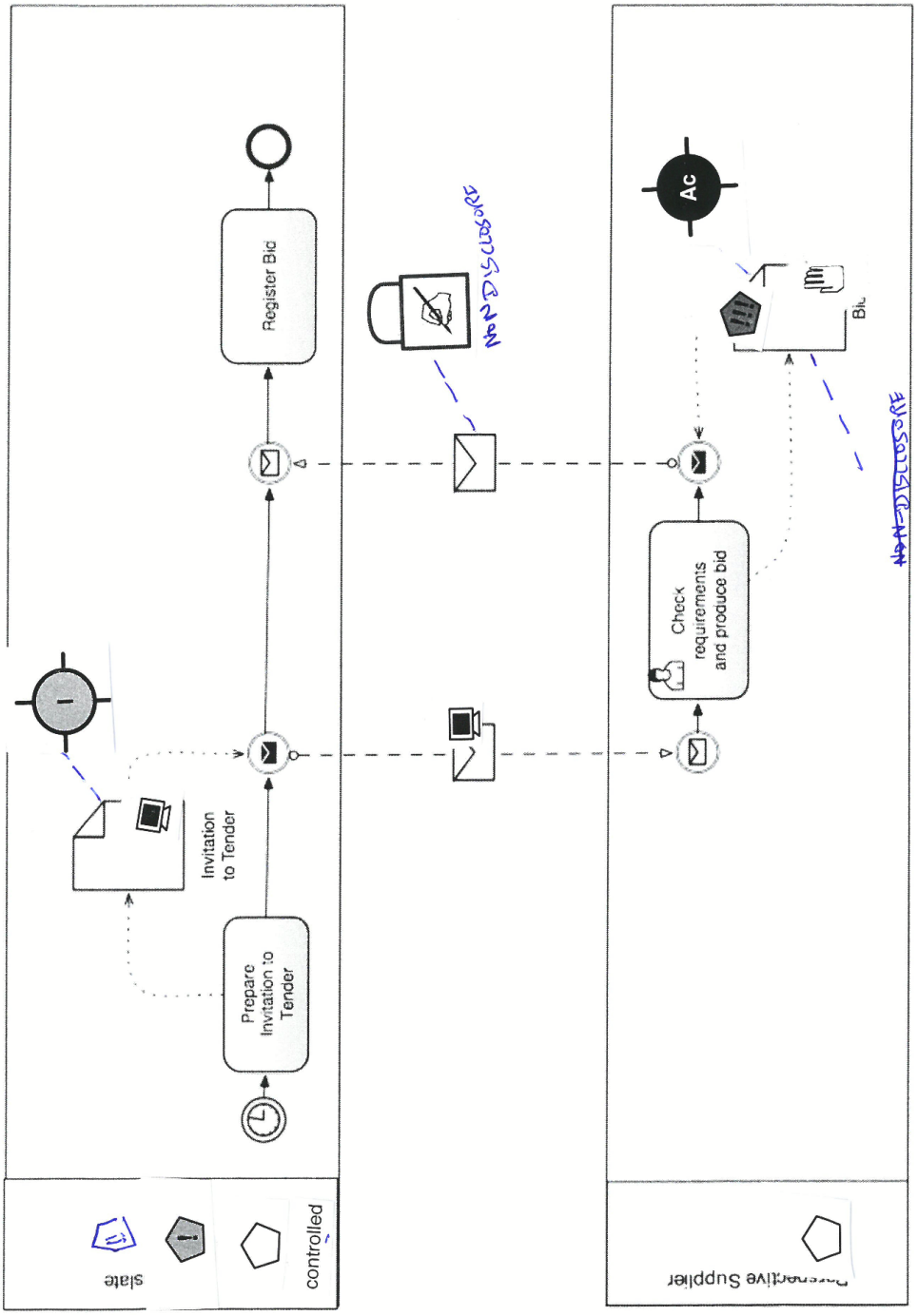


Figure 35: Task 1. Participant 29.

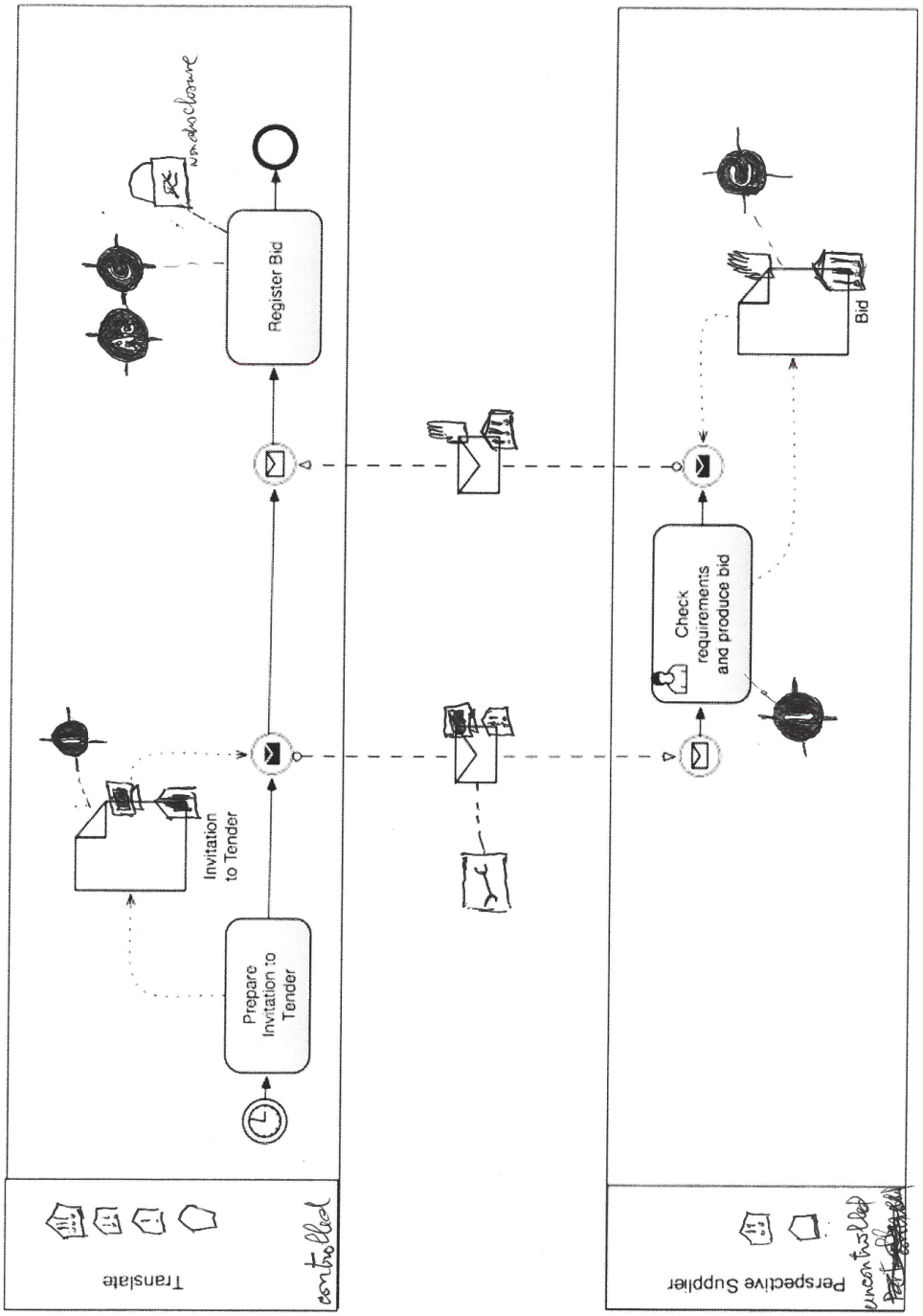


Figure 36: Task 1. Participant 30.

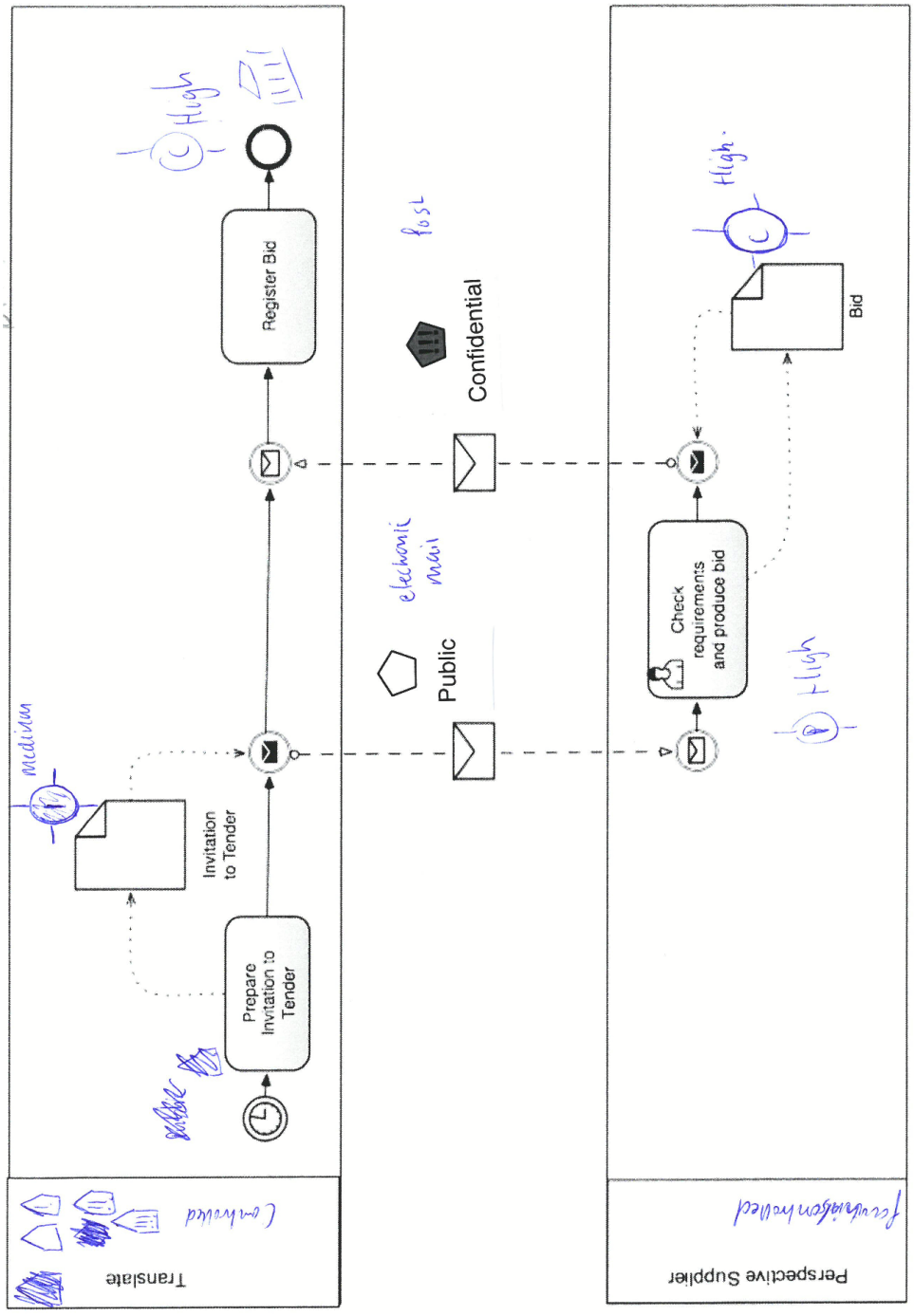


Figure 37: Task 1. Participant 31.

A.22 Secure*BPMN Evaluation. Alternative Hypotheses

Table 12: Hypotheses for testing.

RQ	Hypothesis
RQ1	$H1.1_A$: The mean correctness score of all participants considered together in Task 1 is below 70% and the failure rate is above 5%.
RQ1	$H1.2_A$: The mean correctness score of all participants considered together in Task 2 is below than 70% and the failure rate is above 5%.
RQ1	$H1.3_A$: The mean correctness score of the group of experts in Task 1 is below 70% and the failure rate is above 5%.
RQ1	$H1.4_A$: The mean correctness score of the group of experts in Task 2 is below than 70% and the failure rate is above 5%.
RQ1	$H1.5_A$: The mean correctness score of the group of MSc students in Task 1 is below than 70% and the failure rate is above 5%.
RQ1	$H1.6_A$: The mean correctness score of the group of MSc students in Task 2 is below than 70% and the failure rate is above 5%.
RQ2	$H2.1_A$: There is no difference between the correctness scores of the group of experts and MSc students in Task 1.
RQ2	$H2.2_A$: There is a difference between the correctness scores of the groups of experts and MSc students in Task 2.
RQ3	$H3.1_A$: There is a difference between the time the groups of experts and MSc students spent on Task 1.
RQ3	$H3.2_A$: There is a difference between the time the groups of experts and MSc students spent on Task 2.
RQ4	$H4.1_A$: There is a difference between the correctness scores of Task 1 and Task 2 for the group of experts.
RQ4	$H4.2_A$: There is a difference between the correctness scores of Task 1 and Task 2 for the group of MSc students.
RQ5	$H5.1_A$: There is no correlation between the level of expertise in IAS and performance.
RQ5	$H5.2_A$: There is no correlation between the level of expertise in BPMN and performance.
RQ6	$H6.1_A$: The mean of the PEOU construct of all participants considered together is less than 3.
RQ6	$H6.2_A$: The mean of the PEOU construct of the group of experts is less than 3.
RQ6	$H6.3_A$: The mean of the PEOU construct of the group of MSc students is less than 3.

Continued on the next page

Table 12 – *Continued from the previous page*

RQ	**Hypothesis**
RQ6	$H6.4_A$: The mean of the PU construct of all participants considered together is less than 3.
RQ6	$H6.5_A$: The mean of the PU construct of the group of experts is less than 3.
RQ6	$H6.6_A$: The mean of the PU construct of the group of MSc students is less than 3.
RQ6	$H6.7_A$: The mean of the ItU construct of all participants considered together is less than 3.
RQ6	$H6.8_A$: The mean of the ItU construct of the group of experts is less than 3.
RQ6	$H6.9_A$: The mean of the ItU construct of the group of MSc students is less than 3.
RQ7	$H7.1_A$: There will be a difference between the PEOU of the groups of experts and MSc students.
RQ7	$H7.2_A$: There will be a difference between the PU of the groups of experts and MSc students.
RQ7	$H7.3_A$: There will be a difference between the ItU of the groups of experts and MSc students.

A.23 Secure*BPMN Evaluation. Results

Table 13: Participants' Profiles. Part 1

Partic. No	Country	Role	Level of expertise in business processes	For what purpose do you model business processes
1	UK	Faculty	Quite knowledgable	To understand informationflows and the IAS needs.
2	NLD	Research Director	Quite knowledgeable	Work flow modelling
3	Oman	Manager	Some knowledge	To make everything standard and clear so everyone can follow it
4	Oman	Manager	Some knowledge	not specified
5	Greece	IT Research Student	Some knowledge	not specified
6	UK	Lecturer	Quite knowledgeable	Teaching others to model business processes and representing processes in my research
7	SA	Research Student	Some knowledge	not specified
8	UK	Researcher	Some knowledge	Academic
9	SA	Researcher	Quite knowledgeable	integration of information policies, and domain-specific access control
10	UK	Business Analyst	Some knowledge	Clarity during Requirements Elicitation.
11	UK	Systems Architect	Expert	not specified
12	UK	Policy Maker	Some knowledge	Project Implementation
13	UK	Researcher	Quite knowledgeable	security
14	UK	Consultant	Some knowledge	Consultancy
15	UK	Information Security Framweok, Manager	Quite knowledgeable	business change

Continued on the next page

Table 13 – *Continued from the previous page*

Partic. No	Country	Role	Level of expertise in business processes	For what purpose do you model business processes?
16	UK	InfoSec Program Manager	Some knowledge	informal workflow modeling
17	SA	MSc student	Some	Academic
18	India	MSc student	No knowledge	Academic
19	UK	MSc student	Some knowledge	academic
20	USA	MSc student	Some knowledge	academic
21	UK	MSc student	Some knowledge	Academic
22	UK	MSc student	Some knowledge	Academic
23	UK	MSc student	No knowledge	Academic
24	Greece	MSc student	Some knowledge	Academic
25	India	MSc student	Some knowledge	Academic
26	India	MSc student	No knowledge	Academic
27	Oman	MSc student	No knowledge	Academic
28	UK	MSc student	Some knowledge	Academic
29	UK	MSc student	Some knowledge	Academic
30	UK	MSc student	No knowledge	Academic
31	UK	MSc student	No knowledge	Academic

Table 14: Secure*BPMN Empirical Evaluation. Participants' Profiles. Part 2

Partic. No	Expertise in BPMN	Experience in BPMN	Expertise in IAS	Experience in IAS	Specialisation in IAS
1	Quite knowledgeable	2	Expert	25	Policy, risk management, secure system design and secure operations.
2	No knowledge	0	Expert	13	All except compliance and forensics.
3	No knowledge	0	Quite knowledgeable	3	Cyber Crime, Computer forensics
4	No knowledge	0	Some knowledge	1	Part of management

Continued on the next page

Table 14 – *Continued from the previous page*

Partic. No	Expertise in BPMN	Experience in BPMN	Expertise in IAS	Experience in IAS	Specialisation in IAS
5	No knowledge	0	Some knowledge	10	I'm aware of some InfoSec issues
6	Some knowledge	1	Some knowledge	0	Lecturing in software engineering and system design
7	Some knowledge	1	Quite knowledgeable	6	Privacy
8	Some knowledge	2	Quite knowledgeable	4	Lecturing on InfoSec basic principles
9	Some knowledge	1	Expert	4	InfoSec in healthcare domain
10	Some knowledge	1	Some knowledge	10	Website/application security.
11	Quite knowledgeable	5	Some knowledge	5	not specified
12	Some knowledge	0	Some knowledge	7	Risk Assessment
13	Some knowledge	5	Expert	10	Malware, Risk Assessment
14	Some knowledge	0	Some knowledge	2	Risk Consultancy, System Audit
15	Some knowledge	1	Quite knowledgeable	1	Information Security Management
16	Some knowledge	0	Expert	10	InfoSec coordination
17	No knowledge	0	Some knowledge	0	not specified
18	No knowledge	0	Some knowledge	0	not specified
19	No knowledge	0	Some knowledge	0	not specified
20	No knowledge	0	Some knowledge	0	not specified

Continued on the next page

Table 14 – *Continued from the previous page*

Partic. No	Expertise in BPMN	Experience in BPMN	Expertise in IAS	Experience in IAS	Specialisation in IAS
21	Some knowledge	0	No knowledge	0	not specified
22	Some knowledge	0	No knowledge	0	not specified
23	Some knowledge	0	No knowledge	0	not specified
24	No knowledge	0	Some knowledge	0	not specified
25	Some knowledge	0	No knowledge	0	not specified
26	No knowledge	0	Some knowledge	0.5	Privacy
27	No knowledge	0	Some knowledge	0	not specified
28	No knowledge	0	Some knowledge	0	not specified
29	No knowledge	0	Some knowledge	0	not specified
30	Some knowledge	1	Some knowledge	0	not specified
31	Some knowledge	0	Some knowledge	0.5	InfoSec

Table 15: Task 1. Correctness Results (Table 1 of 2)

Evaluated variable	Location	Access Permissions	Information Format	Information Sensitivity	Security Goal	Criticality	Security Countermeasure	Application Rules	Understanding	Final Score
Participant 1	2	2	2	2	2	2	2	1.75	2	**17.75**
Participant 2	2	2	2	2	2	0	0	0.25	1	**11.25**
Participant 3	2	1.75	2	1	1	1	1	1.5	2	**13.25**
Participant 4	1	1.5	2	0	2	2	1	0.75	0	**10.25**
Participant 5	1	2	2	0	1	1	2	1	2	**12**
Participant 6	1	1.25	2	2	2	2	2	1.5	1	**14.75**
Participant 7	2	2	2	1	2	2	1	1.65	2	**15.65**
Participant 8	2	2	2	2	2	2	2	1.25	2	**17.25**
Participant 9	2	1.5	2	2	2	2	1	1.75	2	**16.25**
Participant 10	2	2	2	2	2	2	1	1.1	2	**16.1**
Participant 11	0	0	2	0	2	2	2	1	1	**10**
Participant 12	1	0.25	2	1	1	0	0	0.75	2	**8**
Participant 13	0	0	2	1	2	2	2	1.25	2	**12.25**
Participant 14	2	0	2	2	2	2	2	1.25	2	**15.25**
Participant 15	0	2	2	2	2	2	2	1.5	2	**15.5**
Participant 16	2	2	2	2	2	2	2	1.9	2	**17.9**

Table 16: Task 1. Correctness Results (Table 2 of 2)

Evaluated variable	Location	Access Permissions	Information Format	Information Sensitivity	Security Goal	Criticality	Security Countermeasure	Application Rules	Understanding	Final Score
Participant 17	1	1.75	2	2	1	1	0	0.75	2	**11.5**
Participant 18	2	1.5	1	0	2	2	2	1.65	1	**13.15**
Participant 19	2	2	2	2	2	2	2	1.75	1	**16.75**
Participant 20	1	1.75	2	2	2	2	2	1.9	2	**16.65**
Participant 21	1	1.75	2	2	2	2	1	1.9	2	**15.65**
Participant 22	1	1.75	2	2	2	2	1	1.35	1	**14.1**
Participant 23	2	0	2	2	2	2	2	1.25	2	**15.25**
Participant 24	2	1.75	2	1	2	2	2	1.8	1	**15.55**
Participant 25	2	1.75	2	2	1	1	0	0.9	1	**11.65**
Participant 26	0	0	1	1	2	2	1	1.25	0	**8.25**
Participant 27	2	0	2	1	2	1	0	0.65	1	**9.65**
Participant 28	1	0	0	2	2	2	0	0.75	0	**7.75**
Participant 29	1	1.75	2	1	2	2	1	1.05	0	**11.8**
Participant 30	2	1.75	2	1	2	1	1	1.75	2	**14.5**
Participant 31	1	1	2	2	1	1	0	0.25	1	**9.25**
Variable average	1.39	1.31	1.87	1.45	1.81	1.65	1.23	1.26	1.42	**13.38**

Table 17: Task 2. Correctness Results (Table 1 of 2)

Evaluated variable	Location	Access Permissions	Information Format	Information Sensitivity	Security Goal	Criticality	Security Countermeasure	Final Score
Partici-pant/Question	Q3+Q12	Q5+Q8	Q4+Q6	Q4 + Q9	Q10 + Q11	Q10 + Q11	Q7+Q13	
Participant 1	1+1	1+1	1+1	1+1	1+1	1+1	1+1	*14*
Participant 2	0+0	1+1	1+1	1+0	0+1	0+1	1+1	*9*
Participant 3	1+1	1+1	0+1	0+1	0+1	0+1	1+1	*10*
Participant 4	0+1	1+1	1+1	1+1	0+1	0+1	1+0	*10*
Participant 5	1+1	1+0	0+1	0+0	0+1	0+1	1+1	*8*
Participant 6	1+1	1+1	0+1	0+1	0+1	0+1	1+1	*10*
Participant 7	1+1	1+1	0+1	0+1	1+1	1+1	1+1	*12*
Participant 8	1+1	1+1	1+1	1+1	1+1	1+1	1+1	*14*
Participant 9	1+1	1+0	1+1	1+1	1+1	1+1	1+1	*13*
Participant 10	1+1	1+1	1+1	1+1	1+1	1+1	1+1	*14*
Participant 11	1+1	1+1	0+1	0+1	0+1	0+1	1+1	*10*
Participant 12	1+0	0+1	1+1	1+1	1+1	1+1	1+1	*12*
Participant 13	1+0	1+1	1+1	1+1	1+1	1+1	1+1	*13*
Participant 14	1+1	1+1	1+0	1+1	1+1	1+1	1+1	*13*
Participant 15	1+1	1+1	1+1	1+1	1+1	1+1	1+1	*14*

Table 18: Task 2. Correctness Results (Table 2 of 2)

Evaluated variable	Location	Access Permissions	Information Format	Information Sensitivity	Security Goal	Criticality	Security Countermeasure	Final Score
Partici-pant/Question	Q3+Q12	Q5+Q8	Q4+Q6	Q4 + Q9	Q10 + Q11	Q10 + Q11	Q7+Q13	
Participant 16	1+1	1+1	1+1	1+1	1+1	1+1	1+1	*14*
Participant 17	1+0	1+0	1+1	1+1	1+1	1+1	1+1	*12*
Participant 18	0+0	0+0	0+0	0+0	0+0	0+0	1+0	*1*
Participant 19	1+1	1+1	1+1	1+1	1+1	1+1	1+0	*13*
Participant 20	1+1	1+0	1+1	1+1	1+1	1+1	1+1	*13*
Participant 21	0+1	1+1	1+1	1+1	1+0	1+0	1+1	*11*
Participant 22	1+0	1+1	1+0	1+1	0+1	0+1	1+0	*9*
Participant 23	1+0	1+0	1+1	1+1	1+1	1+1	1+0	*11*
Participant 24	1+0	1+0	1+1	1+1	0+1	0+1	1+0	*9*
Participant 25	1+0	1+0	1+0	1+0	1+1	1+1	1+0	*11*
Participant 26	1+0	0+0	1+0	1+0	0+1	0+1	1+1	*7*
Participant 27	1+0	1+0	1+1	1+0	0+0	0+0	1+1	*7*
Participant 28	1+0	1+1	1+0	1+1	1+0	1+0	0+0	*8*
Participant 29	1+0	0+1	1+0	1+1	1+1	1+1	1+0	*10*
Participant 30	1+0	1+1	1+0	1+1	0+1	0+1	1+1	*10*
Participant 31	1+0	0+1	1+1	1+1	1+1	1+1	0+1	*11*
Variable average	*1.39*	*1.45*	*1.55*	*1.61*	*1.48*	*1.48*	*1.65*	*10.74*

Table 19: Objective performance metrics

Participant	Time		Correctness Score				Participation
	Task 1 (mins)	Task 2 (mins)	Task 1 (out of 18)	Task 1 (%)	Task 2 (out of 14)	Task 2 (%)	
Participant 1	18	7	17.75	98.61	14	100.00	Remotely
Participant 2	18	4	11.25	62.50	9	64.29	Remotely
Participant 3	15	7	13.25	73.61	10	71.43	In person
Participant 4	18	17	10.25	56.94	10	71.43	In person
Participant 5	16	3	12.00	66.67	8	57.14	In person
Participant 6	23	24	14.75	81.94	10	71.43	In person
Participant 7	18	7	15.65	86.94	12	85.71	In person
Participant 8	15	5	17.25	95.83	14	100.00	Remotely
Participant 9	21	7	16.25	90.28	13	92.86	Remotely
Participant 10	16	7	16.10	89.44	14	100.00	In person
Participant 11	13	12	10.00	55.56	10	71.43	In person
Participant 12	45	15	8.00	44.44	12	85.71	In person
Participant 13	15	10	12.25	68.06	13	92.86	In person
Participant 14	44	15	15.25	84.72	13	92.86	In person
Participant 15	20	6	15.50	86.11	14	100.00	In person
Participant 16	18	5	17.90	99.44	14	100.00	In person
Participant 17	33	5	11.50	63.89	12	85.71	In person
Participant 18	60	10	13.15	73.06	1	7.14	In person
Participant 19	44	7	16.75	93.06	13	92.86	In person
Participant 20	25	5	16.65	92.50	13	92.86	In person
Participant 21	29	7	15.65	86.94	11	78.57	In person
Participant 22	32	12	14.10	78.33	9	64.29	In person
Participant 23	41	15	15.25	84.72	11	78.57	In person
Participant 24	43	8	15.55	86.39	9	64.29	In person
Participant 25	30	10	11.65	64.72	11	78.57	In person
Participant 26	40	9	8.25	45.83	7	50.00	In person
Participant 27	43	3	9.65	53.61	7	50.00	In person
Participant 28	34	10	7.75	43.06	8	57.14	In person
Participant 29	43	8	11.80	65.56	10	71.43	In person
Participant 30	46	11	14.50	80.56	10	71.43	In person
Participant 31	39	12	9.25	51.39	11	78.57	In person
Average	29.52	9.13	13.38	74.35	10.74	76.73	

Table 20: The Shapiro-Wilk test and Levene tests for objective performance metrics.

Participant	Time		Correctness Score	
	Task 1	Task 2	Task 1	Task 2
Experts. Shapiro-Wilk	W = 0.6404, p-value = 3.992e-05	W = 0.8598, p-value = 0.01906	W = 0.9367, p-value = 0.3109*	W = 0.8598, p-value = 0.01904
MSc students. Shapiro-Wilk	W = 0.9373, p-value = 0.3496*	W = 0.9823, p-value = 0.983*	W = 0.9305, p-value = 0.2776*	W = 0.8615, p-value = 0.02534
Levene's Test	F = 0.3177, p-value =0.5773*	F = 1.2627, p-value = 0.2704*	F = 0.0217, p-value = 0.8839*	F = 0.2659, p-value = 0.61*
Chosen Test	Mann-Whitney-Wilcoxon	Mann-Whitney-Wilcoxon	ANOVA	Mann-Whitney-Wilcoxon

* p-value>0.05 - Null hypothesis is accepted.

Null hypothesis of the Shapiro-Wilk test: The population is normally distributed.

Null hypothesis of the Levene's Test: The variances of two populations are equal.

Testing hypothesis H2.1

Descriptives

Score - Task 1

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Min	Max
					Lower Bound	Upper Bound		
Experts	16	77.5681	16.82749	4.20687	68.6014	86.5349	44.44	99.44
MSc students	15	70.9080	16.89892	4.36328	61.5497	80.2663	43.06	93.06
Total	31	74.3455	16.92031	3.03898	68.1391	80.5519	43.06	99.44

ANOVA

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	343.411	1	343.411	1.208	.281
Within Groups	8245.493	29	284.327		
Total	8588.904	30			

Testing hypothesis H2.2

Descriptive Statistics

	N	Mean	Std. Deviation	Minimum	Maximum
Score - Task 2	31	76.7284	19.94651	7.14	100.00
Group	31	1.4839	.50800	1.00	2.00

Mann-Whitney Test. Ranks

Group		N	Mean Rank	Sum of Ranks
Score - Task 2	Experts	16	19.66	314.50
	MSc students	15	12.10	181.50
	Total	31		

Test Statistics[a]

	Score2
Mann-Whitney U	61.500
Wilcoxon W	181.500
Z	-2.335
Asymp. Sig. (2-tailed)	.020
Exact Sig. [2*(1-tailed Sig.)]	.019[b]

a. Grouping Variable: Group b. Not corrected for ties.

Figure 38: The output of hypotheses H2.1 and H2.2 testing

Testing hypothesis H3.1

Descriptive Statistics

	N	Mean	Std. Deviation	Minimum	Maximum
Time - Task 1	31	29.5161	12.82672	13.00	60.00
Group	31	1.4839	.50800	1.00	2.00

Mann-Whitney Test. Ranks

Group		N	Mean Rank	Sum of Ranks
Time - Task 1	Experts	16	10.09	161.50
	MSc students	15	22.30	334.50
	Total	31		

Test Statistics[a]

	Time1
Mann-Whitney U	25.500
Wilcoxon W	161.500
Z	-3.747
Asymp. Sig. (2-tailed)	.000
Exact Sig. [2*(1-tailed Sig.)]	.000[b]

a. Grouping Variable: Group b. Not corrected for ties.

Testing hypothesis H3.2

Descriptive Statistics

	N	Mean	Std. Deviation	Minimum	Maximum
Time - Task 2	31	9.1290	4.58797	3.00	24.00
Group	31	1.4839	.50800	1.00	2.00

Mann-Whitney Test. Ranks

Group		N	Mean Rank	Sum of Ranks
Time - Task 2	Experts	16	15.38	246.00
	MSc students	15	16.67	250.00
	Total	31		

Test Statistics[a]

	Time2
Mann-Whitney U	110.000
Wilcoxon W	246.000
Z	-.399
Asymp. Sig. (2-tailed)	.690
Exact Sig. [2*(1-tailed Sig.)]	.711[b]

a. Grouping Variable: Group b. Not corrected for ties.

Figure 39: The output of hypotheses H3.1 and H3.2 testing

Testing hypothesis H4.1

Descriptive Statistics

	N	Mean	Std. Deviation	Minimum	Maximum
Experts - Task 1 and 2 Scores	32	81.1950	15.98477	44.44	100.00
TaskNo	32	1.5000	.50800	1.00	2.00

Mann-Whitney Test. Ranks

TaskNo		N	Mean Rank	Sum of Ranks
Experts	Task 1	16	14.00	224.00
	Task 2	16	19.00	304.00
	Total	32		

Test Statistics[a]

	Experts - Task 1 and 2 Scores
Mann-Whitney U	88.000
Wilcoxon W	224.000
Z	-1.512
Asymp. Sig. (2-tailed)	.130
Exact Sig. [2*(1-tailed Sig.)]	.138[b]

a. Grouping Variable: TaskNo b. Not corrected for ties.

Testing hypothesis H4.2

Descriptive Statistics

	N	Mean	Std. Deviation	Minimum	Maximum
MSc students - Task 1 and 2 Scores	30	40.4293	31.95317	7.14	92.86
TaskNo	32	1.5000	.50800	1.00	2.00

Mann-Whitney Test. Ranks

TaskNo		N	Mean Rank	Sum of Ranks
MSc students	Task 1	16	10.19	163.00
	Task 2	14	21.57	302.00
	Total	30		

Test Statistics[a]

	Experts - Task 1 and 2 Scores
Mann-Whitney U	27.000
Wilcoxon W	163.000
Z	-3.539
Asymp. Sig. (2-tailed)	.000
Exact Sig. [2*(1-tailed Sig.)]	.000[b]

a. Grouping Variable: TaskNo b. Not corrected for ties.

Figure 40: The output of hypotheses H4.1 and H4.2 testing

Testing hypothesis H6.1-6.9

	N	Mean	Std. Deviation	Std. Error Mean
PU_Experts (H6.5)	16	4.0625	.60539	.15135
PEOU_Experts (H6.2)	16	4.1444	.45525	.11381
ItU_Experts (H6.8)	16	3.5006	.96644	.24161
PU_Students (H6.6)	15	3.9200	.66676	.17216
PEOU_Students (H6.3)	15	4.1553	.76544	.19764
ItU_Students (H6.9)	15	3.3127	.71583	.18483
PU_All (H6.4)	31	3.9935	.62925	.11302
PEOU_All (H6.1)	31	4.1497	.61407	.11029
ItU_All (H6.7)	31	3.4097	.84572	.15190

One sample t-test

	Test Value = 3						
	t	df	Sig. (2-tail) p-value	Sig. (1-tail) p-value	Mean Difference	95% Confidence Interval of the Difference	
						Lower	Upper
PU_Experts (H6.5)	7.020	15	.000	0.000	1.06250	.7399	1.3851
PEOU_Experts (H6.2)	10.055	15	.000	0.000	1.14438	.9018	1.3870
ItU_Experts (H6.8)	2.072	15	.056	0.028	.50063	-.0144	1.0156
PU_Students (H6.6)	5.344	14	.000	0.000	.92000	.5508	1.2892
PEOU_Students (H6.3)	5.846	14	.000	0.000	1.15533	.7314	1.5792
ItU_Students (H6.9)	1.692	14	.113	0.056	.31267	-.0837	.7091
PU_All (H6.4)	8.791	30	.000	0.000	.99355	.7627	1.2244
PEOU_All (H6.1)	10.424	30	.000	0.000	1.14968	.9244	1.3749
ItU_All (H6.7)	2.697	30	.011	0.006	.40968	.0995	.7199

Figure 41: The output of hypotheses H6.1 and H6.9 testing

Testing hypothesis H7.1-7.3

Test of Homogeneity of Variances

	Levene Statistic	df1	df2	Sig.
PU_All	.052	1	29	.821
PEOU_All	1.505	1	29	.230
ItU_All	1.026	1	29	.319

Descriptive Statistics

	N	Mean	Std. Deviation	Minimum	Maximum
PU_All	31	3.9935	.62925	2.40	4.80
PEOU_All	31	4.1497	.61407	2.00	5.00
ItU_All	31	3.4097	.84572	2.00	4.67
Group	31	1.4839	.50800	1.00	2.00

Mann-Whitney Test

Ranks

Group		N	Mean Rank	Sum of Ranks
PU_All	Experts	16	16.31	261.00
	MSc students	15	15.67	235.00
	Total	31		
PEOU_All	Experts	16	15.38	246.00
	MSc students	15	16.67	250.00
	Total	31		
ItU_All	Experts	16	16.97	271.50
	MSc students	15	14.97	224.50
	Total	31		

Test Statistics[a]

	PU_All	PEOU_All	ItU_All
Mann-Whitney U	115.000	110.000	104.500
Wilcoxon W	235.000	246.000	224.500
Z	-.200	-.414	-.635
Asymp. Sig. (2-tailed)	.841	.679	.526
Exact Sig. [2*(1-tailed Sig.)]	.861[b]	.711[b]	.545[b]

a. Grouping Variable: Group

b. Not corrected for ties.

Figure 42: The output of hypotheses H7.1 and H7.3 testing

Table 21: Subjective Perceived Metrics (Part 1 of 2)

Assigned scores: Strongly Disagree - 1; Disagree - 2; Agree - 4; Strongly Agree - 5.

Question	PU1	PU2	PU3	PU4	PU5	PEOU1	PEOU2	PEOU3	PEOU4	ItU1	ItU2	ItU3
Participant 1	5	5	5	4	5	5	5	5	5	5	4	4
Participant 2	4	2	5	5	4	4	5	4	2	4	4	2
Participant 3	4	4	4	5	5	4	5	4	4	5	4	5
Participant 4	2	2	2	2	4	4	4	4	2	2	4	4
Participant 5	5	4	5	5	5	4	4	4	2	5	4	5
Participant 6	5	4	4	5	5	4	4	2	4	2	2	2
Participant 7	4	4	4	4	4	4	2	4	4	2	2	2
Participant 8	4	2	4	5	4	4	4	4	4	4	4	4
Participant 9	5	4	4	5	4	4	4	4	4	4	2	5
Participant 10	5	2	4	5	4	5	5	5	1	2	2	2
Participant 11	4	5	4	4	2	5	4	4	4	4	2	2
Participant 12	4	4	4	4	4	4	4	4	4	4	4	4
Participant 13	4	2	4	4	4	4	4	4	2	4	4	4
Participant 14	4	4	4	4	4	4	4	4	4	4	4	4
Participant 15	5	4	5	5	5	4	5	4	5	5	4	5
Participant 16	4	2	4	4	4	4	5	4	4	4	2	2
Participant 17	5	4	4	5	4	4	4	2	2	4	4	4
Participant 18	4	4	4	4	4	5	5	5	4	4	4	4

Table 22: Subjective Perceived Metrics (Part 2 of 2)

Assigned scores: Strongly Disagree - 1; Disagree - 2; Agree - 4; Strongly Agree - 5.

Question	PU1	PU2	PU3	PU4	PU5	PEOU1	PEOU2	PEOU3	PEOU4	ItU1	ItU2	ItU3
Participant 19	5	2	4	4	4	4	4	4	4	4	2	2
Participant 20	5	2	4	5	4	4	4	4	5	4	2	2
Participant 21	4	2	4	4	4	5	5	4	4	4	2	2
Participant 22	4	4	5	4	4	4	4	4	2	4	4	5
Participant 23	4	4	5	4	4	5	5	5	2	2	2	4
Participant 24	2	2	2	2	4	2	2	2	2	4	2	2
Participant 25	4	4	4	4	4	4	4	4	4	4	4	4
Participant 26	5	4	4	5	4	5	4	4	4	4	4	4
Participant 27	4	5	5	4	5	5	5	5	2	2	4	2
Participant 28	5	4	4	4	4	5	4	4	4	4	4	4
Participant 29	5	4	4	5	4	4	4	4	4	2	4	2
Participant 30	2	2	2	2	4	4	5	5	2	2	2	4
Participant 31	4	4	5	4	4	4	4	4	2	4	4	4
Average Score	4.19	3.39	4.06	4.19	4.13	4.23	4.23	4.00	3.29	3.61	3.23	3.39

Table 23: Subjective performance metrics. Construct scores.

Question	PU	PEOU	ItU
Participant 1	4.80	5.00	4.33
Participant 2	4.00	4.33	3.33
Participant 3	4.40	4.33	4.67
Participant 4	2.40	4.00	3.33
Participant 5	4.80	4.00	4.67
Participant 6	4.60	3.33	2.00
Participant 7	4.00	3.33	2.00
Participant 8	3.80	4.00	4.00
Participant 9	4.40	4.00	3.67
Participant 10	4.00	5.00	2.00
Participant 11	3.80	4.33	2.67
Participant 12	4.00	4.00	4.00
Participant 13	3.60	4.00	4.00
Participant 14	4.00	4.00	4.00
Participant 15	4.80	4.33	4.67
Participant 16	3.60	4.33	2.67
Participant 17	4.40	3.33	4.00
Participant 18	4.00	5.00	4.00
Participant 19	3.80	4.00	2.67
Participant 20	4.00	4.00	2.67
Participant 21	3.60	4.67	2.67
Participant 22	4.20	4.00	4.33
Participant 23	4.20	5.00	2.67
Participant 24	2.40	2.00	2.67
Participant 25	4.00	4.00	4.00
Participant 26	4.40	4.33	4.00
Participant 27	4.60	5.00	2.67
Participant 28	4.20	4.33	4.00
Participant 29	4.40	4.00	2.67
Participant 30	2.40	4.67	2.67
Participant 31	4.20	4.00	4.00

Table 24: Perceived Ease of Use: Number of respondents by the answers provided.

Answer/Item	**PEOU1**	**PEOU2**	**PEOU3**
Strongly Agree (5)	9	11	6
Agree (4)	21	18	22
Disagree (2)	1	2	3
Strongly Disagree (1)	0	0	0

Table 25: Perceived Usefulness: Number of respondents by the answers provided.

Answer/Item	**PU1**	**PU2**	**PU3**	**PU4**	**PU5**
Strongly Agree (5)	12	3	8	12	6
Agree (4)	16	17	20	16	24
Disagree (2)	3	11	3	3	1
Strongly Disagree (1)	0	0	0	0	0

Table 26: Intention to Use: Number of respondents by the answers provided.

Answer/Item	**ItU1**	**ItU2**	**ItU3**
Strongly Agree (5)	4	0	5
Agree (4)	19	12	14
Disagree (2)	8	19	12
Strongly Disagree (1)	0	0	0

A.24 Secure*BPMN Evaluation. Reliability Analysis of Survey Data

Reliability analysis estimates how well the items that reflect the same construct yield similar results. Cronbach's Alpha is a coefficient of internal consistency which shows how consistent the results are for different items for the same construct. In the literature, alphas equal to or greater than 0.7 are considered to be acceptable. The formula for calculating Cronbach's Alpha is as follows [272]:

$$\alpha = \frac{N}{N-1}\left(1 - \frac{\sum_{i=1}^{N} V_i}{V_t}\right), \tag{1}$$

where N is the number of items (e.g. questions) for a construct, V_i is the variance of item scores after weighting, and V_t is the variance of total test scores.

Cronbach's Alpha was calculated for each of three constructs Perceived Usefulness (PU), Perceived Ease of Use (PEOU) and Intention to Use (ItU). For PU and ItU the full set of received answers demonstrated the acceptable level of internal consistency with Cronbach's alphas greater than 0.7 (Table 28).

For the PEOU construct Cronbach's Alpha which is calculated for the original set of responses for four items (PEOU1 - PEOU4) was 0.55. This meant that the results were of low level of internal consistency. To address this the inter-item correlation analysis was conducted for five items of the PEOU construct. The correlation matrix is presented in Table 27. This correlation matrix shows that item PEOU4 does not correlate with PEOU2 and PEOU3. It may indicate a flaw in item PEOU4 (e.g the question was misunderstood by the respondents). In order to achieve the acceptable level of reliability of survey data, it is recommended to drop items with low convergent validity [37]. Therefore, item PEOU4 that has low convergent validity was excluded from the analysis. Cronbach's Alpha which is calculated for three items of the PEOU construct is equal 0.81. Table 28 shows Cronbach's alphas for the constructs and confirms that the level of reliability of all three constructs is acceptable.

Table 27: Correlation matrix for PEOU items.

Item	PEOU1	PEOU2	PEOU3	PEOU4
PEOU1	1			
PEOU2	0.60	1		
PEOU3	0.63	0.56	1	
PEOU4	0.14	-0.0012	0	1

Table 28: Reliability of the Constructs

Construct	Cronbach's alpha
Perceived Ease of Use	0.81
Perceived Usefulness	0.72
Intention to Use	0.71

Bibliography

[1] M. Dlamini, J. Eloff, M. Eloff, "Information security: The moving target," *Computers and Security*, vol. 28, iss. 3-4, May-June 2009, pp. 189-198.

[2] A. Shaw, "Data breach: From notification to prevention using PCI dss," *Columbia Journal of Law and Social Problems*, vol.43(4), pp. 517-562, June 2010.

[3] Sony Computer Entertainment America. Letter to the Subcommittee on Commerce, Manufacturing and Trade of the U.S. House of Representatives. May 3, 2011. [On-line] Available: http://www.flickr.com/photos/playstationblog/sets/72157626521862165 [March 15, 2012].

[4] $(ISC)^2$, The 2011 $(ISC)^2$ Global Information Security Workforce Study. 2011 [On-line] Available: https://www.isc2.org/uploadedFiles/Industry_Resources/FS_WP_ISC20Study_020811_MLW_Web.pdf [February 15, 2012].

[5] Gartner, Inc. Forecast Overview: Security Infrastructure, Worldwide, 2010-2016, 2Q12 Update. 2012.

[6] PwC. Information Security Breaches Survey 2014. Technical report, 2014.

[7] Y. Cherdantseva and J. Hilton, "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals," In: *Organizational, Legal, and Technological Dimensions of Information System Administrator*. F. Almeida and I. Portela, Eds. IGI Global Publishing, 2013, pp. 167-198.

[8] M. Dark, J. Ekstrom and B. Lunt, "Integration of Information Assurance and Security into the IT2005 Model Curriculum," In: SIGITE '05 Proceedings of the 6th conference on Information technology education. ACM, NY, USA, 2005, pp. 7-14.

[9] M. Weske. OpenHPI course on Business Process Modeling and Analysis. 2013 [On-line]. Available: https://open.hpi.de/courses/bpm2013 [December, 2013].

[10] A. Van Looy, "Business process maturity. A comparative study on a sample of business process maturity models," Ph.D. dissertation, Ghent University, 2012.

[11] W. Van der Aalst, "A Decade of Business Process Management Conferences: Personal Reflections on a Developing Discipline Business Process Management," In: Proceedings of 10th International Conference BPM 2012. LNCS, vol. 7481, Springer, Heidelberg, 2012, pp. 1-16.

[12] J. Becker, M. Rosemann, C. von Uthmann, "Guidelines of business process modeling," In: *Business Process Management: Models, Techniques and Empirical Studies*, W. van der Aalst, J. Desel, A. Oberweis, Eds., Springer-Verlag, Berlin, 2000, pp.30-49.

[13] S. Gopalakrishnan and G. Sindre. Analytical Evaluation of Notational Adaptations to Capture Location of Activities in Process Models. Technical report M3W-1, Department of Computer and Information Science Norwegian University of Science and Technology, August 2011.

[14] A. Rodrìguez, E. Fernández-Medina, ‚J. Trujillo, M. Piattini, "Secure business process model specification through a UML 2.0 activity diagram profile," *Decision Support Systems*, 51(3), 2011, pp. 446-465.

[15] W. van der Aalst, "Process-aware information systems: Lessons to be learned from process mining," *Transactions on Petri Nets and Other Models of Concurrency II*. Springer Berlin Heidelberg, 2009, pp. 1-26.

[16] J. Mendling, H. A. Reijers, and J. Recker, "Activity labeling in process modeling: Empirical insights and recommendations," Inf. Syst., vol. 35/4, Jun. 2010, pp. 467-482.

[17] M. Weske, *Business Process Management: Concepts, Languages, Architectures.* 2nd ed. Springer, 2012.

[18] C. Liu, Q. Li, X. Zhao, "Challenges and opportunities in collaborative business process management: Overview of recent advances and introduction to the special issue," *Information Systems Frontiers*, 11(3), 2009, pp. 201-209.

[19] E. Paja, P. Giorgini, S. Paul, P. Meland, "Security Requirements Engineering for Secure Business Processes," In: *Workshops on Bus. Informatics Research.* L. Niedrite, R. Strazdina, B. Wangler, Eds. LNBIP, vol. 106, Springer, 2012, pp.77-89.

[20] Y. Alotaibi, "Business process modelling challenges and solutions: a literature review." *Journal of Intelligent Manufacturing*, 2014, pp. 1-23.

[21] J. Mulle, S.Stackelberg, K. Bőhm, "A Security Language for BPMN Process Models," Karlsruhe Reports in Informatics 2011,9. Edited by Karlsruhe Institute of Technology, Faculty of Informatics. ISSN 2190-4782, 2011.

[22] A. Goldstein, U. Frank, "A Language for Multi-Perspective Modelling of IT Security: Objectives and Analysis of Requirements." In: *Business Process Management Workshops*, Springer Berlin Heidelberg, 2013, pp. 636-648.

[23] J. Dehnert, W. Aalst, "Bridging the gap between business models and workflow specifications," *Int. J. Cooperative Inf. Syst.*, vol. 13, no. 3, 2004, pp. 289-332.

[24] A. Rodríguez, E Fernández-Medina, M. Piattini, "A BPMN Extension for the Modeling of Security Requirements in Business Processes," I*EICE - Trans. Inf. Syst.*, vol. E90-D, 2007, pp. 745-752.

[25] O. Altuhhova, R. Matulevičius, N. Ahmed, "Towards Definition of Secure Business Processes," In: *Advanced Information Systems Engineering Workshops*, vol. 112, Springer, 2012, pp. 1-15.

[26] Y. Cherdantseva, J. Hilton, O. Rana, "Towards SecureBPMN - Aligning BPMN with the Information Assurance & Security Domain," In: *Business Process Model and Notation 2012*, J. Mendling and M. Weidlich, Eds., LNBIP, vol.125, Springer, Heidelberg, 2012, pp.107-115.

[27] S. Alter, "Defining information systems as work systems: implications for the IS field," *European Journal of Information Systems*, 17(5), 2008, pp. 448-469.

[28] M. Whitman and H. Mattord, *Principles of Information Security*, 4th edition, Course Technology, Cengage Learning, 2012.

[29] T. Neubauer, M. Klemen, S. Biffl, "Secure business process management: A roadmap," Availability, Reliability and Security, 2006. The First International Conference on. IEEE, 2006, p.8.

[30] D. Moody, "The "Physics" of notations: Toward a scientific basis for constructing visual notations in software engineering," *Software Engineering*, IEEE Transactions on, 35(6), 2009, pp. 756-779.

[31] N. Genon, P. Heymans, D. Amyot, "Analysing the cognitive effectiveness of the BPMN 2.0 visual notation," *Software Language Engineering*, Springer Berlin Heidelberg, 2011, pp. 377-396.

[32] Y. Cherdantseva and J. Hilton, "The Survey of Information Security and Information Assurance Professionals," In: *Organizational, Legal, and Technological Dimensions of Information System Administrator*, F. Almeida, I. Portela, Eds., IGI Global Publishing, 2013, pp. 243-256.

[33] K. Järvelin and T. Wilson, "On conceptual models for information seeking and retrieval research", *Information Research*, 9(1), 2003, pp. 163.

[34] Y. Wand and R. Weber, "An Ontological Model of an Information System," I*EEE Transactions on Software Engineering*, 16, 1990, pp. 1282-1292.

[35] S. Graeme, E. Tansley, R. Weber, "Using ontology to validate conceptual models." *Communications of the ACM* 46.10, 2003, pp. 85-89.

[36] Y. Wand, V. C. Storey, R. Weber, "An ontological analysis of the relationship construct in conceptual modeling," *ACM Trans. Database Syst*, 24(4), 1999, pp. 494-528.

[37] D. Moody, "The method evaluation model: a theoretical model for validating information systems design methods," . In *ECIS 2003 Proceedings*, 2003, p. 79.

[38] A. Brucker, I. Hang, G. Lückemeyer, R. Ruparel, "SecureBPMN: Modeling and Enforcing Access Control Requirements in Business Processes," In: ACM symposium on access control models and technologies SACMAT, ACM Press, 2012, pp. 123-126.

[39] Collins English Dictionary Online, http://www.collinsdictionary.com.

[40] Oxford Dictionaries Online, http://oxforddictionaries.com.

[41] J. Sherwood, A. Clark, D. Lynas, *Enterprise Security Architecture: A Business-Driven Approach*. CMP Books, 2005.

[42] D. Pipkin, *Information Security: Protecting the global enterprise.* Hewlett-Packard Company, 2000.

[43] J.S. Tiller, *Adaptive Security Management Architecture*. Auerbach Publications, 2010

[44] R. Anderson, "Why Information Security is Hard ? An Economic Perspective," Computer Security Applications Conference, ACSAC 2001. Proc. 17th Annual, 2001, pp. 358-365.

[45] B. Schneier, *Schneier on Security*. Wiley Publishing. 2008.

[46] D.Lacey, *Managing the Human factor in information security*. J. Wiley and Sons Ltd., 2009.

[47] B. Von Solms, "Information Security - a multidimentional discipline," *Computers & Security*, vol: 20(6), Elsevier, 2001, pp: 504-508.

[48] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, "The insider threat to information systems and the effectiveness of ISO17799," *Computers & Security*, 24, 2005, pp. 472-484.

[49] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley Publishing, 2001.

[50] ISACA, "An Introduction to the Business Model for Information Security," 2009.

[51] Shoemaker, D., Bawol, J., Drommi, A., et al., A Delivery Model for an Information Security Curriculum. In Proceedings of the Third Security Conference, (Las Vegas, Nevada, USA), Information Institute, 2004.

[52] Jerico Forum (JF). The What and Why of De-perimeterization. Available online at http://www.opengroup.org/jericho/deperim.htm [accessed on 16.04.2011].

[53] U.S. Department of Defense (DOD). Directive Number 8500.01E October 24, 2002. Certified Current as of April 23, 2007.

[54] Y. Cherdantseva, O. Rana, J. Hilton, "Security Architecture in a Collaborative De-Perimeterised Environment: Factors of Success", ISSE Securing Electronic Business Processes, Prague 22-23 November 2011. Highlights of the ISSE 2011 Conference, pp. 201-213

[55] ISO/IEC 27000:2009 (E) *Information technology - Security techniques - Information security management systems - Overview and vocabulary*.

[56] CNSS (Committee on National Security Systems), *National Information Assurance (IA) Glossary*, CNSS Instruction No. 4009, 26 April 2010.

[57] ISACA. Glossary of Terms, 2008.

[58] S. Röhrig, Using Process Models to Analyse Security Requirements, Phd. Thesis, University of Zurich, 2003.

[59] N. Mayer, Model-based Management of Information System Security Risk, Phd. Thesis, University of Namur, 2009.

[60] C. Wolter, M. Menzel, C. Meinel, "Modelling Security Goals in Business Processes," Proc. GI Modellierung 2008, GI LNI 127, Berlin, Germany, 2008, pp. 197-212.

[61] D. Parker, "Our Excessively Simplistic Information Security Model and How to Fix It", *ISSA Journal*, July 2010, pp. 12-21.

[62] CSIA. *A National Information Assurance Strategy.* Crown, 2007.

[63] NIST. Risk Management Guide for Information Technology Systems. Special Publication 800-30. July 2002.

[64] IT Governance Institute (ITGI). COBIT 4. Excerpt. 2007.

[65] J. McCumber, "Information Systems Security: A Comprehensive Model," In Proceeding of the 14th National Computer Security Conference, NIST, Baltimore, MD, October, 1991.

[66] D. Parker. "Fighting Computer Crime." NY: J. Wiley and Sons, 1998.

[67] D. Firesmith, "Specifying reusable security requirements." *Journal of Object Technology*, 3.1, 2004, pp. 61-75.

[68] A. Ekelhart, S. Fenz, M. Klemen, E. Weippl, "Security Ontology: Simulating Threats to Corporate Assets," In: Information Systems Security, LNCS, A. Bagchi, V. Atluri, Eds., vol. 4332, Springer, 2006, pp. 249-259.

[69] ISO/IEC 27002:2005, "Information technology - Security techniques - Code of practice for information security management".

[70] Information Assurance Collaboration Group (IACG). Industry Response To The HMG Information Assurance Strategy and Delivery Plan. A report by the IACG Working Group On The Role Of Industry In Delivering The National IA Strategy (IWI009). 2007.

[71] Information Assurance Advisory Council (IAAC) in association with Microsoft. Benchmarking Information Assurance. 2002.

[72] Shoemaker, D., Bawol, J., Drommi, A., et al., A Delivery Model for an Information Security Curriculum. In Proceedings of the Third Security Conference, (Las Vegas, Nevada, USA), Information Institute, 2004.

[73] Chahino, M. and Marchant, J. CIS conference presentation, Washington DC. 2010.

[74] M. Kazemi, H. Khajouei and H. Nasrabadi. Evaluation of information security management system success factors: Case study of Municipal organization. African Journal of Business Management Vol. 6(14), pp. 4982-4989, 2012.

[75] D. E. Bell and L. La Padula, "Secure Computer System: Unified Exposition and Multics Interpretation", ESD-TR-75-306, ESD/AFSC, Hanscom AFB, Bedford, MA 01731, 1975.

[76] D. Clark and D. Wilson, "A Comparison of Commercial and Military Computer Security Policies", in Proc. IEEE Symposium on Security and Privacy, 1987, pp.184-195.

[77] K. Biba, "Integrity Considerations for Secure Computer Systems", ESD-TR-76-372, ESD/AFSC, Hanscom AFB, Bedford, MA, Apr. 1977.

[78] M. R. Clarkson and F. B. Schneider, Hyperproperties. *Journal of Computer Security*, 18(6), 2010, pp. 1157-1210.

[79] C. Blanco, J. Lasheras, E. Fernández-Medina, R. Valencia-García, and A. Toval, "Basis for an integrated security ontology according to a systematic review of existing proposals," *Computer Standards & Interfaces*, 33(4), 2011, pp. 372-388.

[80] M. Sabbari and H. Alipour, "A Security Model and its Strategies for Web Services," *International Journal of Computer Applications*, 36.10, 2011.

[81] Oracle. Information Security: A conceptual architecture approach. April 2011

[82] S. Ransbotham and S. Mitra, "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," *Information Systems Research*, 20(1), 2009, pp.121-139.

[83] J. Corbin, A. Strauss, "Grounded theory research: Procedures, canons and evaluative criteria," *Qualitative Sociology*, 13(1), 1990, pp. 3-21.

[84] Vermeulen, Clive, and Rossouw Von Solms. "The information security management toolbox - taking the pain out of security management." *Information Management & Computer Security*, 10(3), 2002, pp. 119-125.

[85] K. Kumar, "Information Security Management for Governments", ISACA Journal, 4, 2011.

[86] W. Maconachy, C. Schou, D. Ragsdale, D. Welch, "A Model for Information Assurance: An Integrated Approach," In Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, U.S. Military Academy, West Point, NY, 5-6 June, 2001.

[87] D. Trček, "An integral framework for information systems security management." *Computers & Security*, 22(4), 2003, pp. 337-360.

[88] R. Saint-Germain, "Information security management best practice based on ISO/IEC 17799," *Information Management Journal*, 39(4), 2005, pp. 60-66.

[89] M. Dark, N. Harter, L. Morales, M. Garcia, "An information security ethics education model," *Journal of Computing Sciences in Colleges*, 23(6), 2008, pp. 82-88.

[90] W. Al-Hamdani, "Non-risk assessment information security assurance model," in InfoSecCD '09, Information Security Curriculum Development Conference, Kennesaw, GA, USA, 2009.

[91] H. Mouratidis, P. Giorgini, G. Manson, "Integrating security and systems engineering: Towards the modelling of secure information systems," *Advanced Information Systems Engineering*, Springer, 2003, pp. 10-31.

[92] C. Reed, "Legally Binding Electronic Documents: Digital Signatures and Authentication," *The International Lawyer*, Vol. 35, 2001, pp. 89-106.

[93] X. Lu, "Information assurance conception model and applications for largescale information systems," Signal Processing, 2006 8th International Conference on., Vol. 4. IEEE, 2006.

[94] J. Saltzer and M. Schroeder, "The protection of information in computer systems", Proceedings of the IEEE 63 (9), 1975, pp. 1278-1308.

[95] E. Jonsson, "Towards an integrated conceptual model of security and dependability," Availability, Reliability and Security, The First International Conference on. IEEE, 2006, p. 8.

[96] Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance & Security," In Availability, Reliability and Security (ARES), Eighth International Conference on, IEEE, 2013, pp. 546-555.

[97] R. E. Slavin, "Best-Evidence Synthesis: An Alternative to Meta-Analytic and Traditional Reviews," *Educational Researcher*, 15(9), 1986, pp. 5-11.

[98] P. Fettke and P. Loos, "Perspectives on Reference Modeling," in P. Fettke & P. Loos (eds.) *Reference Modeling for Business Systems Analysis*, Idea Group, 2007, pp. 1-20.

[99] D. Moody, "Theoretical and practical issues in evaluating the quality of conceptual models: Current state and future directions," *Data Knowl. Eng.*, vol. 55(3), 2005, pp. 243-276.

[100] OASIS, "Reference Model for Service Oriented Architecture", OASIS Standard version 1.0 , 12 October 2006.

[101] J.F. Sowa and J.A. Zachman, "Extending and formalizing the framework for information systems architecture." *IBM systems journal*, 31(3), 1992, pp. 590-616.

[102] BS ISO/IEC 10746-1:1998 *Information technology. Open distributed processing. Reference model. Overview.*

[103] U. Frank, "Evaluation of Reference Models," in P. Fettke & P. Loos (eds.) *Reference Modeling for Business Systems Analysis*, Idea Group, 2007.

[104] R. Davis, H. Shrobe, and P. Szolovits, "What is a Knowledge Representation?" *AI Magazine*, 14(1), 1993, pp. 17-33.

[105] NIST, Information Security Handbook: A Guide for Managers, NIST Special Publication 800-100. October, 2006.

[106] ISO/IEC 12207:2008(E) IEEE Std 12207 - 2008 *Systems and software engineering - Software life cycle processes*.

[107] W. McKnight, "What is information assurance?" CrossTalk, *The Journal of Defense Software Engineering,* 2002, pp. 4-6.

[108] The Jerico Forum. Information Classification. [Online] Available: https://collaboration.opengroup.org/jericho/COA_Information Classification_v1.0.pdf. [May 11, 2012]

[109] HMG. HMG Security policy framework. 1 May 2010.

[110] Cabinet Office. Government Security Classifications. Version 1.0. April 2014.

[111] OECD. Development of policies for protection of critical information infrastructures. Ministerial background report DSTI/ICCP/REG(2007)20/FINAL. 2007.

[112] Homeland Security. Supplemental tool: Connecting to NICC and NCCIC. [Online] Available: http://www.dhs.gov/sites/default/files/publications. [January 30, 2014].

[113] Official website of the Department of Homeland Security. Traffic Light Protocol (TLP) Matrix. [Online] Available:http://www.us-cert.gov/tlp/. [January 30, 2014].

[114] BS ISO/IEC 27001:2005 - *Information technology - Security techniques - Information security management systems - Requirements*.

[115] Sarbanes-Oxley Act of 2002. Pub. L. 107-204. 116 Stat. 745.

[116] BS ISO/IEC 27005:2011 - *Information technology. Security techniques. Information security risk management.*

[117] FIPS PUB 199. Standards for Security Categorization of Federal Information and Information Systems. February 2004.

[118] C. Alberts, A. Dorofee, J. Stevens, C. Woody, Introduction to the OCTAVE Approach. Software Engineering Institute. August 2003.

[119] D. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, G. Sussman, "Information accountability," *Communications of the ACM*, 51(6), 2008, pp. 82-87.

[120] D. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, G. Sussman, "Information accountability." Computer Science and Artificial Intelligence Laboratory. Technical Report MIT-CSAIL-TR-2007-034 June 13, 2007.

[121] FRC (Financial Reporting Council), Internal Control: Revised Guidance for Directors on the Combined Code. October 2005.

[122] P. Neumann, *Computer-Related Risks*. ACM Press. 1995.

[123] FRC. The Turnbull guidance as an evaluation framework for the purposes of Section 404(a) of the Sarbanes-Oxley Act.

[124] King Committee on Corporate Governance, Executive Summary of King Report 2002. Institute of Directors in South Africa. 2002.

[125] OECD. OECD Principles of Corporate Governance. OECD Publications Service, 2004.

[126] Foreword by W.Ware in C. Pfleeger and S. Pfleeger, *Security in Computing*, 4th ed. Prentice Hall, 2006.

[127] S. Mason, *Electronic Signatures in Law*, 3rd ed., Cambridge: Cambridge University Press, 2012, pp.229-231; 318-322.

[128] R.Smith and J. Shao, "Privacy and e-commerce: a consumer-centric perspective," *Electronic Commerce Research*, 7(2), 2007, pp. 89-116.

[129] S.D Warren and L.D. Brandeis, "The right to privacy [the implicit made explicit," *Harvard Law Review*, 4(5), 1890, pp. 193-220.

[130] OECD, Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, OECD Digital Economy Papers, No. 178, OECD Publishing. 2011.

[131] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 2012.

[132] M. Quinn, *Ethics for the Information Age*, Pearson/Addison-Wesley Boston 2005.

[133] H. Almagwashi, and A. Gray, "Preserving Privacy in E-government: A System Approach," In: Proceedings of IFIP EGOV2012, Kristiansand, Norway, 2012.

[134] Facebook. Privacy. [Online] Available: https://www.facebook.com/help/445588775451827 [March 15, 2014].

[135] I. Winkler and B. Dealy, "Information security technology?... Don't rely on it. A case study in social engineering," Proceedings of the 5th Unix Security Symposium. The usenix Association, 1995.

[136] D. Moody, "The method evaluation model: a theoretical model for validating information systems design methods," ECIS 2003 Proceedings, ECIS. 2003. pp. 79.

[137] ISO/IEC 13335-1:2004 - *Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*. Status: Withdrawn.

[138] SANS. Information Security Policy - A Development Guide for Large and Small Companies. SANS Institute. 2007.

[139] R. Green, *The Persuasive Properties of Color*, Marketing Communications. 1989.

[140] P. M. Lester, Syntactic Theory of Visual Communication. Online Available: http://commfaculty.fullerton.edu/lester/writings/viscomtheory.html [March 15, 2013].

[141] C. Willis and S. Miertschin, "Mind maps as active learning tools." *Journal of Computing Sciences in Colleges*, 21(4), 2006. pp. 266-272.

[142] BS ISO 7010:2011 - *Graphical symbols. Safety colours and safety signs. Registered safety signs.*

[143] Ockham's razor. Encyclopedia Britannica Online. [Online] Available: http://www.britannica.com/EBchecked/topic/424706/Occams-razor. [June 12, 2013].

[144] A. Antón, J. Earp, A. Reese, "Analyzing website privacy requirements using a privacy goal taxonomy." *Requirements Engineering*, Proceedings. IEEE Joint International Conference on. IEEE, 2002, pp.23-31.

[145] M. Hughes, *The voice of Prophets*. Volume 2 of 12. Morrisville, North Carolina: Lulu.com., 2005, pp. 590-591.

[146] M. Mayers and M. Newman, "The Qualitative Interview in IS Research: Examining the Craft," *Information and Organization*, 17, 2007, pp. 2-26.

[147] I. Benbasat, D. Goldstein, M. Mead, "The Case Research Strategy in Studies of Information Systems," *MIS Quarterly*, 11, 1987, pp. 369-388.

[148] L. Chung and B. Nixon, "Dealing with non-functional requirements: three experimental studies of a process-oriented approach," Software Engineering, ICSE. 17th International Conference on. IEEE, 1995.

[149] D. Moody and G. Shanks, "What makes a good data model? Evaluating the quality of entity relationship models," In Proceedings of the 13th International Conference on the Entity-Relationship Approach, Manchester, UK, 1994, pp. 94-111.

[150] R v Bow Street Magistrates Court and Allison (AP) Ex parte Government of the United States of America (Allison). 2 AC 216. 1999.

[151] B. Blakley, E. McDermott, D. Geer, "Information Security is Information Risk Management," In Proceedings of the 2001 workshop on New Security Paradigms NSPW '01. ACM, NY, USA, 2001, pp. 97-104.

[152] M. Salnitri, F. Dalpiaz, P. Giorgini, "Modeling and verifying security policies in business processes," *Enterprise, Business-Process and Information Systems Modeling*. Springer Berlin Heidelberg, 2014, pp. 200-214.

[153] P. Trkman, "The critical success factors of business process management," *International Journal of Information Management*, 30(2), 2010, pp. 125-134.

[154] M. Weske, W. van der Aalst, H. Verbeek, "Advances in business process management," *Data & Knowledge Engineering*, 50(3), 2004, pp. 1-8.

[155] J.-N. Gillot, *The complete guide to business process management. Business process transformation or a way of aligning the strategic objectives of the company and the information system through the processes*. South Carolina: Booksurge Publishing. 2008.

[156] S. Forster, J. Pinggera, B. Weber, "Collaborative Business Process Modeling." *EMISA*, vol. 206, 2012, pp. 81-94.

[157] B. List, B Korherr, "An evaluation of conceptual business process modelling languages." Proceedings of the 2006 ACM symposium on Applied computing. ACM, 2006, pp. 1532-1539.

[158] W. Curtis, M. I. Kellner, J. Over, "Process Modeling," *Communications of the ACM*, Vol. 35, No. 9, 1992, pp. 75-90.

[159] J. Recker, "Opportunities and constraints : the current struggle with BPMN," *Business Process Management Journal*, 16(1), 2010, pp. 181-201.

[160] The OMG, Business Process Model and Notation (BPMN) Version 2.0, 2011-01-03. [Online] Available: http://www.omg.org/spec/BPMN/2.0 [June 10, 2013].

[161] ISO/IEC 19510:2013(E) - *Information technology - Object Management Group Business Process Model and Notation*.

[162] J. Recker, M. Indulska, M. Rosemann, P. Green, "How Good is BPMN Really? Insights from Theory and Practice," 14th European Conference on Information Systems, Goeteborg, Sweden: Association for Information Systems, 2006, pp. 1582-1593.

[163] S. White, "Using BPMN to Model a BPEL Process," *BPTrends*, 2005, 3(3), 2005, pp. 1-18.

[164] C. Wolter and A Schaad, "Modeling of Task-Based Authorization Constraints in BPMN", in BPM '07: Proceedings of the 5th International Conference on Business Process Management, 2007, pp. 64-80.

[165] T. Wahl, G. Sindre, "An analytical evaluation of BPMN using a semiotic quality framework," *Advanced topics in database research*, vol. 5, 2006, p. 94.

[166] G. Monakova, A. Brucker, A. Schaad, "Security and safety of assets in business processes," In: Proceedings of the 27th Annual ACM Symposium on Applied Computing, ACM, 2012, pp. 1667-1673.

[167] J. Recker, M. Rosemann, "A measurement instrument for process modeling research : development, test and procedural model," *Scandinavian Journal of Information Systems*, 22(2), 2010, pp. 3-30.

[168] H. Volzer, "An Overview of BPMN 2.0 and its Potential Use," In: 2nd International Workshop BPMN, Potsdam, Germany. 2010.

[169] D. Peixoto, V. Batista, A. Atayde, E. Borges, R. Resende, and C. Pádua, "A comparison of BPMN and UML 2.0 activity diagrams," VII Simposio Brasileiro de Qualidade de Software, Vol. 56. 2008.

[170] A.G. Nysetvold, J. Krogstie, "Assessing Business Process Modeling Languages Using a Generic Quality Framework," In Proceedings of the CAiSE'05 Workshops, J. Castro, E. Teniente, Eds., vol. 1, 2005, pp. 545-556.

[171] D. Birkmeier, S. Kloeckner, S. Overhage, "An empirical comparison of the usability of BPMN and UML activity diagrams for business users," *ECIS 2010 Proceedings*, Paper 51, 2010.

[172] OMG. Unified Modeling LanguageTM (OMG UML), Infrastructure. Version 2.4.1. [Online] Available: http://www.omg.org/spec/UML/2.4.1/Infrastructure. [January 24, 2013].

[173] B. Marcinkowski, M. Kuciapski, "A business process modeling notation extension for risk handling," *Computer Information Systems and Industrial Management*, Springer Berlin Heidelberg, 2012, pp. 374-381.

[174] É. Dubois, P. Heymans, N. Mayer, R. Matulevičius, "A Systematic Approach to Define the Domain of Information System Security Risk Management," *Intentional Perspectives on Information Systems Engineering*, Springer, 2010, pp. 289-306.

[175] S. Jakoubi, S. Tjoa, G. Goluch, G. Quirchmayr, "A Survey of Scientific Approaches Considering the Integration of Security and Risk Aspects into Business Process Management," In: Database and Expert Systems Application, 2009. DEXA'09, 20th International Workshop on, IEEE, 2009, pp. 127-132.

[176] M. Riesner, G. Pernul, "Supporting compliance through enhancing internal control systems by conceptual business process security modeling," In: Proceedings of the 21st Australasian Conference on Information Systems (ACIS), 2010, pp. 1-10.

[177] M. Leitner, M., Miller, S. Rinderle-Ma, "An Analysis and Evaluation of Security Aspects in the Business Process Model and Notation," In: Availability, Reliability and Security (ARES) 2013, Eighth International Conference on, IEEE, 2013, pp. 262-267.

[178] M. Leitner, S. Rinderle-Ma, "A systematic review on security in Process-Aware Information Systems-Constitution, challenges, and future directions," *Information and Software Technology*, 56(3), 2014, pp. 273-293.

[179] A. Saleem, "Qualitative Study of Domain Specific Languages for Model Driven Security," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 7(17), 2014, pp. 3514-3521.

[180] S. Suriadi, B. Weiss, A. Winkelmann, A. ter Hofstede, M. Wynn, C. Ouyang, A. Pika, "Current research in risk-aware business process management-overview, comparison, and gap analysis." BPM Center Report BPM-12-13, BPMcenter.org, 2012.

[181] M. Menzel, I. Thomas, C. Meinel, "Security requirements specification in service-oriented business process management," In: Proceedings of International Conference on Availability, Reliability and Security, ARES'09. IEEE, 2009, pp. 41-48.

[182] C. Wolter, M. Menzel, A. Schaad, P. Miseldine, C. Meinel, "Model-driven business process security requirement specification," *Journal of Systems Architecture*, 55(4) 2009, pp. 211-223.

[183] A. Varela-Vaca, R. Gasca, A. Jimenez-Ramirez, "A Model-Driven engineering approach with diagnosis of non-conformance of security objectives in business process models," In: RCIS, Fifth International Conference on, IEEE, 2011, pp. 1-6.

[184] M. Saleem, J. Jaafar, M. Hassan, "A Domain-Specific Language for Modelling Security Objectives in a Business Process Models of SOA Applications", AISS: *Advances in Information Sciences and Service Sciences*, Vol. 4(1), 2012, pp. 353- 362.

[185] O. Altuhhova. R. Matulevičius, N. Ahmed, "An Extension of Business Process Model and Notation for Security Risk Management," International Journal of Information System Modeling and Design, vol. 4(4), 2013, pp. 93-113.

[186] A. Souza, B. Silva, F. Lins, J. Damasceno, N. Rosa, P. Maciel, C Northfleet, "Incorporating security requirements into service composition: From modelling to execution," *Service-Oriented Computing*. Springer Berlin Heidelberg, 2009, pp. 373-388.

[187] J. Mulle, S. von Stackelberg, K. Bohm, "Modelling and transforming security constraints in privacy-aware business processes," Service-Oriented Computing and Applications (SOCA), IEEE International Conference on. IEEE, 2011, pp.1-4.

[188] C. Wheildon, *Type and Layout: Are You Communicating or Just Making Pretty Shapes?*, Hastings, Victoria, Australia: Worsley Press, 2005.

[189] M. Rekik, K. Boukadi, H. Ben-Abdallah, "BPMN metamodel extension with deployment and security information," The 13 International Arab Conference on Information Technology, ACIT, 2012, pp. 611-617.

[190] J. Hilton, A. Tawileh, "Sustained Control of Critical Corporate Information," 5th Middle East Chief Information Officer Conference & IT Exhibition, ME CIO 2008. Summit, 2008, Bahrain [Online]. Available: http://www.jeremy-hilton.com/node/1 [July 30, 2011].

[191] Y. Wand, R. Weber, "On the Ontological Expressiveness of Information Systems Analysis and Design Grammars," Journal of Information Systems, 3 (4), 1993, pp. 217-237.

[192] A. Blackwell, C. Britton, A. Cox, T. Green,C. Gurr, G. Kadoda, R. Young, "Cognitive dimensions of notations: Design tools for cognitive technology," In: Cognitive Technology: Instruments of Mind, ser. LNCS. Springer,no. 2117, 2001, pp. 325-341.

[193] N. Goodman, *Languages of art: An approach to a theory of symbols*. Hackett publishing, 1976.

[194] H. Reijers, J. Mendling, "A study into the factors that influence the understandability of business process models," Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, 41(3), 2011, pp. 449-462.

[195] I. Vanderfeesten, J. Cardoso, J. Mendling, H. Reijers, W. van der Aalst, "Quality metrics for business process models," *BPM and Workflow handbook*. vol. 144. Future Strategies Inc. 2007, pp. 179-190.

[196] G. Miller, "The magical number seven, plus or minus two: some limits on our capacity for processing information," *Psychological review*, vol 63(2), 1956, p. 81.

[197] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, Vol. 13(3), 1989, pp. 319-340.

[198] Cardiff University. *Cardiff Centre for Lifelong Learning. Student Handbook 2013-2014*. [Online] Available: http://www.cardiff.ac.uk/learn/assets/PDF/LLL-Handbook(E).pdf [September 2, 2014].

[199] K. Pearson, "Notes on regression and inheritance in the case of two parents," Proceedings of the Royal Society of London, 58, June 20, 1895, pp. 240-242.

[200] N. Salkin, *Encyclopedia of Measurement and Statistics*. SAGE Publications, Inc. 2007.

[201] K. Labunets, F. Massacci, F. Paci, L. Tran, "An experimental comparison of two risk-based security methods," Empirical Software Engineering and Measurement, 2013 ACM/IEEE International Symposium on. IEEE, 2013, pp. pp. 163-172.

[202] K. Labunets, F. Paci, F. Massacci, R. Ruprai,"An experiment on comparing textual vs. visual industrial methods for security risk assessment. Empirical Requirements Engineering (EmpiRE), 2014 IEEE Fourth International Workshop on. IEEE, 2014, pp. 28-35.

[203] W3C. OWL 2 Web Ontology Language Document Overview. 2009.

[204] H. Mouratidis, P. Giorgini, G. Manson, I.Philp, "A Natural Extension of Tropos Methodology for Modelling Security," Proceedings Agent Oriented Methodologies Workshop, Annual ACM Conference on Object Oriented Programming, Systems, Languages (OOPSLA), Seattle - USA, 2002.

[205] F. Ulrich, "Multi-perspective enterprise modeling (memo) conceptual framework and modeling languages," System Sciences, in Proc. 35th Annual Hawaii International Conference on. IEEE, 2002, pp. 1258-1267.

[206] National Computer Security Center (NCSC). Integrity in Automated Information Systems. C Technical Report 79-91 Library No. S-237,254(IDA PAPER P-2316). September 1991.

[207] B. Schneier, *Secrets and Lies*. John Wiley and Sons, 2000.

[208] NIST. Risk Management Guide for Information Technology Systems. Special Publication 800-30. July 2002.

[209] L. Gordon, M. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, Vol. 5(4), November 2002, pp. 438-457.

[210] Jerico Forum (JF). The What and Why of De-perimeterization. Available online at http://www.opengroup.org/jericho/deperim.htm [accessed on 16.04.2011]

[211] Jericho Forum (JF). Jericho Forum Commandments. 2007.

[212] Joint Pub 3-13. Joint Doctrine for Information Operations. USA, 1998.

[213] The Cabinet Office. HMG Information Assurance Maturity Model and Assessment Framework. Crown Copyright. Version 4.0, 27 May 2010.

[214] A. Tawileh and S. McIntosh, "Understanding Information Assurance: A Soft Systems Approach," Proceedings of the United Kingdom Systems Society 11th International Conference, September 3-5, 2007, Oxford University, UK.

[215] A. Shostack "The evolution of information security" in The Next Wave: Developing a blueprint for a science of cybersecurity, vol. 19(2) 2012.

[216] ISO/IEC 15408-1:2009 - *Information technology-Security techniques-Evaluation criteria for IT security. Part 1: Introduction and general model.*

[217] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1. Revision 3. July 2009.

[218] The Cabinet Office. HMG Security Policy Framework. v.5.0, Crown Copyright. Feb 2011.

[219] The author started a discussion about the origins of the CIA-triad on the LinkedIn, in the Information Security Community Group. R. Leo, one of the authors of the term CIA-triad participated in the discussion and explained his insight on the CIA-triad.

[220] R. von Rössing, "Applying BMIS to Cloud Security," in: ISSE 2010 Securing Electronic Business Processes, 2010, pp. 101-112.

[221] N. Findler, *Associative networks: The representation and use of knowledge by computers*. Academic Press, Inc., 1979.

[222] C. Landwehr, "Cybersecurity: From engineering to science," *Developing a blueprint for a science of cybersecurity*, 2012, p. 2.

[223] J. Anderson, "Why we need a new definition of information security," *Computers & Security*, 22(4), 2003, pp. 308-313.

[224] A. Avizienis, J.Laprie, B. Randell, and C. E. Landwehr, Basic concepts and taxonomy of dependable and secure computing. IEEE Trans. Dependable Sec. Comput., vol. 1, no. 1, pp. 11-33, 2004

[225] H. Venter and J. Eloff, "A taxonomy for information security technologies," Computers & Security, 22(4), 2003, pp.299-307.

[226] PD ISO/IEC TR 24748-1:2010 - *Systems and software engineering - Life cycle management. Part 1: Guide for life cycle management.*

[227] BS ISO/IEC 13335-3:2004 - *Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security*.

[228] NIST. Glossary of Key Information Security Terms. IR 7298. Revision 1. R. Kissel, Ed., February 2011.

[229] F. Gallegos, "Red Teams: An Audit Tool, Technique and Methodology for Information Assurance," ISACA Journal Online, 2006 ISACA, pp. 1-4. [Online] Available: http://www.isaca.org/Journal/Past-Issues/2006/Volume-2/Documents/jpdf0601-red-teams-audit-tool.pdf [June 16, 2013].

[230] J. Sherwood, A. Clark, D. Lynas, "SABSA. Enterprise Security Architecture", White Paper. SABSA Limited. 2009.

[231] G. Peterson, Security Architecture Blueprint. Arctec Group, LLC. 2007.

[232] N. Mayer, P. Heymans and R. Matulevičius, "Design of a modelling language for information system security risk management," in Proceedings of the 1st International Conference on Research Challenges in Information Science (RCIS 2007), 2007, pp.121-131.

[233] Microsoft. Security Development Lifecycle. [Online] Available: http://www.microsoft.com/security/sdl/default.aspx [September 3, 2012]

[234] A. Herzog, N. Shahmehri, C. Duma, "An ontology of information security," *International Journal of Information Security and Privacy* (IJISP) 1(4), 2007, pp. 1-23.

[235] J. Anttila, J. Kajava and R. Varonen, "Balanced Integration of Information Security into Business Management," in Proceedings of the 30th EUROMICRO Conference, 2004, pp.558-564.

[236] The U.S. Joint Staff (JS). Information Assurance through Defense in Depth. February 2000.

[237] Copyright, Designs and Patents Act 1988. c. 48. [Online] Available: http://www.legislation.gov.uk/ukpga/1988/48 [March 4, 2012].

[238] S. Jakoubi, S. Tjoa, S. Goluch, G. Kitzler, "Rsk-Aware Business Process Management-Establishing the Link Between Business and Security," *Complex Intelligent Systems and Their Applications*, 2010, pp.109-135.

[239] Pavlovski, Christopher J., and Joe Zou. "Non-functional requirements in business process modeling," Proceedings of the fifth Asia-Pacific conference on Conceptual Modelling-Volume 79. Australian Computer Society, Inc., 2008.

[240] Bocciarelli, Paolo, and Andrea D'Ambrogio. "A BPMN extension for modeling non functional properties of business processes." Proceedings of the 2011 Symposium on Theory of Modeling & Simulation: DEVS Integrative M&S Symposium. Society for Computer Simulation International, 2011.

[241] Saeedi, Kawther, Liping Zhao, and Pedro R. Falcone Sampaio. "Extending BPMN for supporting customer-facing service quality requirements." Web Services (ICWS), 2010 IEEE International Conference on. IEEE, 2010.

[242] D. Basin, J. Doser, T. Lodderstedt, "Model driven security for process-oriented systems," In: Proceedings of the 8h ACM Symposium on Access Control Models and Technologies (SACMAT), ACM, New York, USA, 2003, pp. 100-109.

[243] J. Jürjens, "UMLsec: extending UML for secure systems development," Proceedings of the 5th International Conference on UML - The Unified Modeling Language, vol. 2460, Springer, 2002, pp. 412-425.

[244] M. Hafner, M. Breu, R. Breu, A. Nowak, "Modelling inter-organizational workflow security in a peer-to-peer environment," In: Proceedings of the IEEE International Conference on Web Services (ICWS), 2005, pp. 533-540.

[245] M. Hafner, R. Breu, Realizing model driven security for inter-organizational workflows with WS-CDL and UML 2.0, in: Proceedings of the 8th International Conference on Model Driven Engineering Languages and Systems (MoDELS), Lecture Notes in Computer Science, vol. 3713, Springer, 2005, pp. 39-53.

[246] M. Decker, An UML profile for the modelling of mobile business processes and workflows, in: Proceedings of the 5th International Conference on Mobile Multimedia Communications (MobiMedia), ACM, Kingston upon Thames, UK, 2009, pp. 38:1-38:7.

[247] D. Domingos, A. Rito-Silva, P. Veiga, Workflow access control from a business perspective, in: Proceedings of the 6th International Conference on Enterprise Information Systems (ICEIS), vol. 3, 2004, p. 18-25.

[248] J. McDermott, "Abuse-Case-Based Assurance Arguments,"In: Proc. of the 17th Annual Comp. Security Applications Conf., IEEE Computer Society, 2001, pp. 366.

[249] J. McDermott, C. Fox, "Using Abuse Case Models for Security Requirements Analysis," In: Proceedings of ACSAC'99, IEEE Computer Society, 1999, pp. 55.

[250] I. Soomro, A. Naved, "Towards security risk-oriented misuse cases," Business Process Management Workshops. Springer Berlin Heidelberg, 2013, pp. 689-700.

[251] G. Goluch, A. Ekelhart, S. Jakoubi, S. Tjoa, T., Mück, "Integration of an Ontological Information Security Concept in Risk Aware Business Process Management," In: Proceedings of the 41st Hawaii International Conference on System Sciences, HICSS2008, 2008, pp. 377-385.

[252] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl, "Security Ontologies: Improving Quantitative Risk Analysis," in Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS 2007), Jan 2007, p. 156.

[253] A. Rodríguez, E. Fernández-Medina, M. Piattini, "Towards a UML 2.0 Extension for the Modeling of Security Requirements in Business Processes," *Trust and Privacy in Digital Business*, Springer, 2006, pp.51-61.

[254] OMG. UML Profile for Modeling QoS and Fault Tolerance Characteristics and Mechanisms [Online] Available: http://www.omg.org/spec/QFTP/1.1, 2009. [March 4, 2013].

[255] A. Naved, R. Matulevičius, "Securing business processes using security risk-oriented patterns," *Computer Standards & Interfaces*, 36(4), 2014, pp. 723-733.

[256] OMG Staff Strategy Group. Model Driven Architecture. White Paper. Draft 3. November 27, 2000.

[257] OMG. MDA Guide Version 1.0.1 2003 [Online] Available: http://www.omg.org/cgi-bin/doc?ormsc/2001-07-01. [January 26, 2012].

[258] D. Basin, D. Jürgen, T. Lodderstedt, "Model driven security: From UML models to access control infrastructures," *ACM Transactions on Software Engineering and Methodology* (TOSEM), 15(1), 2006, pp. 39-91.

[259] R. Breu, M. Hafner, B. Weber, A. Novak, "Model driven security for inter-organizational workflows in e-government," *E-Government: Towards Electronic Democracy,* Springer Berlin Heidelberg, 2005, pp. 122-133.

[260] M. Clavel, V. da Silva,C. Braga, M. Egea, "Model-driven security in practice: An industrial experience," *Model Driven Architecture - Foundations and Applications*. Springer Berlin Heidelberg, 2008, pp. 326-337.

[261] J. Recker, M. Rosemann, P. Green, M. Indulska, "Extending the scope of representation theory: a review and a proposed research model," In 3rd Biennial ANU Workshop on Information Systems Foundations, ANU E-Press, 2007, p. 93.

[262] R. Weber, *Ontological Foundations of Information Systems*. Coopers & Lybrand and the Accounting Association of Australia and New Zealand, Melbourne, Australia, 1997.

[263] S. Espaná, N. Condori-Fernandez, A. González, Ó. Pastor, "An empirical comparative evaluation of requirements engineering methods," *Journal of the Brazilian Computer Society*, 16(1), 2010, pp. 3-19.

[264] B. Fabian, S. GÃ$\frac{1}{4}$rses, M. Heisel, T. Santen, H. Schmidt, "A comparison of security requirements engineering methods," *Requirements engineering*, 15(1), 2010, pp. 7-40.

[265] S. Jamieson, "Likert scales: how to (ab) use them," *Medical education* 38(12), 2004, pp. 1217-1218.

[266] R. Armstrong, "The midpoint of a five-point Linkert-type scale," *Perceptual and Motor Skills*, vol. 64, 1987, pp. 359-362.

[267] R.Garland, "The mid-point on a rating scale: Is it desirable," *Marketing Bulletin*, vol. 2(1), 1991, pp. 66-70.

[268] ISO/IEC 27010:2012 *Information technology. Security techniques. Information security management for inter-sector and inter-organizational communications*.

[269] A. Avizienis, J.-C. Laprie, B. Randell, C. E. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Dependable Sec. Comput.*, 1(1), 2004, pp. 11-33.

[270] J. Boyce, D. Jennings, *Information Assurance: Managing Organizational IT Security Risks*. Butterworth-Heinemann. Elsevier Science, 2002.

[271] E. Jonsson, "An integrated framework for security and dependability," in: Workshop on New security paradigms, ACM, 1998, pp. 22-29.

[272] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," *Psychometrika*, 16(3), 1951, pp. 297-334.