

Effective Communication of Information Security Risk

**Aseela Nasser Al Harthi
PhD 2019**



Effective Communication of Information Security Risk

Aseela Nasser Al Harthi

2019

Cardiff University

School of Computer Science & Informatics

**A thesis submitted in partial fulfilment of the requirement
for the degree of Doctor of Philosophy**

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 it being submitted concurrently in candidature for any degree or other awards.

Signed ...[Aseela Al Harthi](#)..... (candidate)

Date ...[14th October, 2019](#).....

STATEMENT 1

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

Signed [Aseela Al Harthi](#) (candidate)

Date[14th October, 2019](#).....

STATEMENT 2

This thesis is the result of my own independent work/investigation, except where otherwise stated, and the thesis has not been edited by a third party beyond what is permitted by Cardiff University's Policy on the Use of Third Party Editors by Research Degree Students. Other sources are acknowledged by explicit references. The views expressed are my own.

Signed [Aseela Al Harthi](#)..... (candidate)

Date ...[14th October, 2019](#).....

STATEMENT 3

I hereby give consent for my thesis, if accepted, to be available online in the University's Open Access repository and for inter-library loan, and for the title and summary to be made available to outside organisations.

Signed [Aseela Al Harthi](#) (candidate)

Date[14th October, 2019](#).....

Dedication

*With a grateful heart, I would like to dedicate this research to my beloved parents, **Nasser Al Harthi** and **Saleema Al Harthi**, for their endless love, support and care for me since day one of my life; without this I would not be able to do or achieve anything in life. Your valuable advice to read the following ayah enlightens my path all the time.*

"O my Lord! Let my entry be by the Gate of Truth and Honour, and likewise my exit by the Gate of Truth and Honour; and grant me from Thee an authority to aid (me)."

(Holy Quraan 017.080)

To my Husband, Salim Al Mataani, your patience, love, kindness and care helped me a lot to work hard and do my best.

To my little angels, Omar, Shahm and AlReem.

To every member of my family for their support which helped make my work easier. I thank Allah for blessing me with such a wonderful family. Without their love and encouragement, I might not have completed this research thesis. I'm so grateful for all those times you stood by me, believing in me and giving me faith and confidence that I can reach my goal.

To my lovely country Oman.

I hope I made you all proud.

I love you all.

Abstract

Cloud computing enables location-independent access to data and plays a significant role in a “linked-up” healthcare environment. Having cloud computing can improve the availability of patient medical records but there is the need to have the right processes in place to realise the benefits of cloud-enabled services. Potential benefits include rapid provisioning and interconnectivity of electronic resources to enhance data availability, and big data analytics help analyse patient data to provide the right intervention to the right patient at the right time through linking the collaboration and communication among healthcare institutions in different locations. Assunção et al. (2015) provided a vision that cloud computing would become the fifth utility, which will offer essential computing services for daily use.

Despite the known benefits of cloud computing, the Ministry of Health (MoH) in Oman is hesitant to adopt cloud computing in patient services in healthcare because of perceived risks. There is therefore the need to understand the perception of different types of risks in adopting cloud computing in healthcare in Oman, such as security, management, technical, legal, privacy and other types of risks. To this end, a preliminary interview was conducted with stakeholders and two sets of questionnaires were issued to public and healthcare professionals in order to understand their perception of the risks in adopting cloud computing as a service in healthcare. The findings identified data security, confidentiality, integrity and availability as primary concerns. Therefore, an effective methodology is required to manage those concerns.

This research focuses on information security risk management within the healthcare industry. It introduces a methodology, Managing Security Risk-Business Process Modelling (MSR-BPM), as an approach to manage the identified risks. The MSR-BPM approach is built on ISO 27005 processes to help organisations prioritise, manage and treat the identified risks. The primary purpose is to enhance the communication of information security risk in healthcare processes, which can be improved by combining risk registers and business process modelling. A risk register documents the assessment of risk with appropriate countermeasures. BPM visualises the risks, activities, roles, security goals and countermeasures in the process models to promote a shared understanding of risks to decision makers and stakeholders.

Finally, the MSR-BPM approach was evaluated through a scenario covering stages in the Integrated Care Pathway for breast cancer. This scenario was chosen because it has been used by previous researchers within the School of Computer Science and Informatics at Cardiff University. An evaluation that covered the set of ISO 27005 processes was produced to create a survey for experts in risk management, business process modelling and healthcare. The experts agreed that combining risk registers with business process modelling improved the communication of information security risk in healthcare processes when compared to using risk registers only.

Acknowledgment

How can I thank you enough!

First of all, praise and thanks be to God for countless blessings and virtues which provided me with the opportunity to step into the fascinating world of research and thanks for granting me the capability and strength to successfully pursue my PhD. Thank you so much for giving me more than I could ask for and so, God, let the knowledge that you have granted me be useful for myself and others. Let it be an argument for me and not against me.

The PhD journey has been a hard, excruciating, but also very rewarding experience. At times, I felt as if I was swimming in rough seas or climbing high mountains as I tried to maintain my focus to achieve my research aims. I'm indebted to many people who have helped me to reach the top of this mountain and enjoy the beautiful scenery.

I am heartily grateful and thankful to my supervisors, Dr. Wendy Ivins and Prof. Omer Rana, for their encouragement, advice and continuous support that enlightened me throughout this research. I thank Allah for having excellent supervisors like you who hold knowledge and expertise in research. I feel lucky to be under your supervision, as I could not have done it without your constructive comments, support and good advice during our discussions. Also, I would like to thank Dr. Yulia Cherdantseva for the wonderful discussions and support that enabled the research to move in the right direction. I am also grateful to all the staff at the School of Computer Science & Informatics for their unconditional help whenever it was needed. Special thanks to Dr. Rob Davies and Ms Helen Williams.

I am forever grateful to Prof. Keith G. Jeffery and Dr. Omnia Allam for their invaluable feedback and great support. Prof. Jeffery, Dr. Allam, Thank you!

I would also like to convey my thanks to his Majesty Sultan Qaboos bin Said for granting the Makramah Scholarship through the Ministry of Higher Education for ambitious Omani students to pursue their postgraduate studies. I feel lucky to have been accepted, enabling me to pursue my dream to complete my PhD study. Also, I would like to thank my home university, Sultan Qaboos University, for releasing me to embark upon my studies. I also express my appreciation to all my colleagues back

home in the College of Economics and Political Science for their moral support: Dr. Fahim Almarhubi, Dr. Zakia AlAdawi, Dr. Faris Al Said, Mrs. Kareema Alamri, Mrs. Nourah Al Hosni and Mrs. Fatmah Al Busaidi.

Also, I would like to thank Dr. Sara Al Bahlani for correcting the translation from English to Arabic for two sets of questionnaires and Ms. Gill Scrimgeour for patiently proofreading my thesis and providing supportive words as if you were standing in my shoes. You have been very thoughtful and caring.

In addition, I would like to extend my sincere thanks to Dr. Hessah Al Salamah, Dr. Shada Al Salamah, Dr. Omnia Allam and Dr. Alysia Skilton as their PhD theses helped me to understand the clinical side of the hypothetical healthcare scenario and apply Business Process Model to it. Dr. Shada, thank you so much for encouraging to me to participate in the Saudi conference.

I wish to express my deepest gratitude to members of my dear family, special thanks to my dear bother Mr. Nasr Al Harthi and Mrs. Amal Al Harthi for dedicating time to discuss my work and find connections to conduct preliminary interviews at the initial stage of my research regardless of the long and busy schedule with your own work. You committed to helping me with a kind smile and supportive words. Also, special thanks to my dear sister, Ph. Aisha Al Harthi, who encouraged me to participate in the Oman conference and dedicated time to ease the process for me and my family. Moreover, thanks to my dear brother, Mr. Rashid Al Harthi, and his wife, Mrs. Haleema Al Kyiomi, for giving me support and help when I had my little angel, Shahm, during my PhD journey. Also, my dear brother Mr. Salim Al Harthi and his wife Mrs. Jehad Al Mataani as well as my dear brother, Mr. Abdullah Al Harthi and his wife Bushra Al Habsi and dear sister Ms. Sara Al Harthi for travelling back and forth to give me support and encouragement to continue my trip. Also, my sister Mrs. Bushra Al Harthi, thank you so much for your moral support. I'm really blessed to have a wonderful and supportive family like you. I wish you all success in your careers.

In addition, very special thanks to my aunt Mayya Al Harthi for taking care of my son

Omar during the first year. It was the hardest thing I have ever done in my life. Also, thanks and appreciation is due to my family-in-law; Ms. Ibtisam Al Mutaani, Ahmed Al Mutaani, Said Al Mutaani, Talal Al Mutaani, Anwar Al Mutaani, Bader Al Mutaani and Taha Al Mutaani. You have all been supportive and encouraging and may Allah ease your path with a successful future. Also, I would like to thank all my family members who helped me in circulating my survey. With your help, I managed to obtain a useful number of participants. Thank you so much. Moreover, I would like to extend my thanks to all participants who spared some time to complete the survey. Likewise, I would like to thank the managers who gave up their valuable time to answer and discuss interview questions with me.

Furthermore, I would like to express my deep appreciation and gratefulness to my best friend and soul mate, Dr. Asma Al-Zaidi, who shared her experience and knowledge with me to analyse the data. Your forward thinking helped me a lot to narrow my focus to specify the results I needed. I cannot thank you enough for your help and support whenever I needed it. I'm really lucky to have you as a sister and close friend to my heart.

Also, I would like to gratefully thank Dr. Saqib Ali who encouraged me to complete my PhD journey and helped me out whenever I needed his advice. You are very supportive and may Allah reward you with health and wealth En Sha Allah. I also wish to extend my thanks to my best friends in Oman, Mrs. Nada Al Kiyoumi, Mrs. Alia Al Busaidi, Mrs. Maha Al Amri and Ms. Manal Abdulsamad. You are very supportive and caring. I miss our great times together and keep telling myself that one day I will come back home, and meet you all again.

Moreover, high appreciation is due to my fellow doctoral students; those who have moved on, those in the quagmire, and those just beginning, who helped me by providing a welcome ear to listen to my thoughts during the hard times and tried to help by sharing a discussion from the first year onwards; Dr. Neelam Memon, Mrs. Warda Al Habsi, Mrs. Shahd Alahdal and Ms. Asma Alshuhail. I really appreciate your time and effort to help as well as your encouragement and optimistic words that the hard times will pass. I'm heartily grateful for the kind support of Shahd; you are a very dear friend. Special thanks to Ms. Asma for providing an opportunity to refresh my brain with fresh air by walking to get a coffee in the middle of the day. Also, Dr.

Soha Ahmed Ehssan for supportive words and showing me the facilities within our building; this was so helpful. Also, I would like to thank and recognise the moral support and encouragement from Dr. Asma Al Saida and Dr. Haya Almagwashi. Similarly, big thanks my fellow doctoral students; Mrs.Wafa Alorainy, Mrs. Enas Alradaddi, Mrs. Karma Albalawi, Dr. Ashwan Abdulmunem, Ms. Khtam Al-Meyah, Mrs. Shelan Jeawak, Dr. Liqaa Nawaf, Dr. Fatma Alrayes, Mrs. Rana Al Shekh, Mrs. Alanoud Subahi, Dr. Louise Knight, Ms. Lucie Lèvêque and Ms. Majedah Alrehiely for the encouraging and supportive words during our gatherings on different occasions.

Finally, I would like to extend the deepest gratitude and my heartfelt thanks to my beloved grandmother, Mama Fatmah, who never really understood why I always had to be away from home and sadly passed away before I managed to submit my thesis. I remember your prayers and best wishes. I have to say that I could not complete my PhD journey without the support of my loving and caring family, my mother who gladly travelled to the UK many times to support me and look after my children, my very supportive husband Salim who always encouraged my career and fully appreciated the hard times I experienced during this journey. My children, Omar, Shahm and AlReem, who do not have an interest in Information Security Risk Management; however, they graciously accepted me leaving them for long hours as Mum has to work hard to finish important research. Your presence inspired, touched and illuminated my heart during my PhD journey.

From this long journey, I believe that I have gained the resilience to face any situation in life: *“Resilience is the ability to work with adversity in such a way that one comes through it unharmed or even better for the experience. Resilience means facing life’s difficulties with courage and patience – refusing to give up”* (Wisdom Commons, 2018).

Thank you all so much; I’m blessed and will be forever grateful.

Aseela Nasser Al Harthi
Cardiff, UK
2019

List of Acronyms

AAA	Authorisation Authentication Auditing
BPM	Business Process Modelling
BS	British Standard
C.I.A.	Confidentiality, Integrity and Availability
CaNISC	Cancer Network Information System
CC	Cloud Computing
CEHR	Cloud-based Electronic Health Records
CIS	Clinical Information Systems
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information Technology for governance framework
CP	Cloud Provider
CRR	Corporate Risk Register
CSDDRLT	Consolidating and Standardizing the Database of Diagnosis, Radiology and Laboratory Tests
CT	Care Team
DR	Disaster Recovery
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
EFA	Exploratory Factor Analysis
EHR	Electronic Health Record
ENISA	European Union Agency for Network Information Security
EPR	Electronic Patient Record
EU	Europe Union
EVAR	Endovascular Aneurysm Repair
FAM	Federation Access Management
FMEA	Failure Modes and Effect Analysis
FTA	Fault Tree Analysis

GDPR	General Data Protection Regulation
GH	Germany Hospital
GP	General Practitioner
HER	Health Electronic Records
HFME	Health Failure Mode Effect Analysis
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
HL7	Health Level Seven
IaaS	Infrastructure as a Service
IAS	Information Assurance and Security
ICD-10-CM	International Classification of Diseases, Tenth Revision, Clinical Modification
ICP	Integrated Care Pathway
ICT	Information and Communication Technology
IoT	Internet of Things
ISDLC	Information System Development Life Cycle
ISMS	Information Security Management Systems
ISO 19510	Information Technology-Object Management Group Business Process Model and Notation
ISO 20000	Information Technology Service Management System
ISO 25010	Quality Model Requirement SQuaRE
ISO 27001	Information Security Management Systems
ISO 27005	Information Security Risk Management
ISO 27799:2008	Health informatics -Information security management in health using ISO/IEC 27002
ISO 27799:2016	Health informatics -Information Security Management in health using ISO/IEC 27002
ISO 31000	Risk Management Standard
ISO 38500	Corporate Governance of Information Technology
ISPD	Information Security Policy Document
ITA G-Cloud	Information Technology Authority- Government-Cloud

ITA	Information Technology Authority
ITA-Cloud	Information Technology Authority-Cloud
ITIL	Information Technology Infrastructure Library
M_o_R®	Management of Risks
MDT	Multi-Disciplinary Team
MHMS	M-Health monitoring system
MoH	Ministry of Health in Oman
MoNE	Ministry of National Economy
MSR-BPM	Managing Security Risk-Business Process Model
NCPS	National Centre for Patient Safety
NCSI	National Centre for Statistics & Information
NDA	Non-Disclosure Agreement
NHS	National Health Service
NIS	National Inpatient Sample
NIST	National Institute of Standards and Technology
OCTAVE	Operational Critical Threat and Vulnerability Evaluation
OH	Oman Hospital
PaaS	Platform as a Service
PACS	Picture Archiving and Communication Systems
PC	Patient-Centred
PCIDSS	Payment Card Industry Data Security Standard
PDCA	Plan-Do-Check-Act model
PHE	Personal Health Record
PHI	Protected Health Information
PKI	Primary Key Infrastructure
PMBOK	Project Management Body of Knowledge
RA	Risk Analysis
RIS	Radiological Information Systems
RMG	Risk Management Group
RMIAS	Reference Model of Information Assurance and Security
RR	Risk Register
SaaS	Software as a Service

SecSDLC	Security System Development Lifecycle
SHarE	Secure Healthcare Collaborative Environment
SLA	Service Level Agreement
SoA	Service-Oriented Architecture
SPISCDDRLT	Selection and Purchase of International Standards for Connecting Databases and Diagnostic Radiology and Laboratory Tests
TOGAF	The Open Group Architecture Framework
U.S.	United States
WBAN	Wireless Body Area Network
WfICP	Workflow for Integrated Care Pathway
WHO	World Health Organization

Table of Contents

<i>DECLARATION</i>	<i>v</i>
<i>Dedication</i>	<i>ix</i>
<i>Abstract</i>	<i>xi</i>
<i>Acknowledgment</i>	<i>xiii</i>
<i>List of Acronyms</i>	<i>xvii</i>
<i>Table of Contents</i>	<i>xxi</i>
<i>List of Figures</i>	<i>xxviii</i>
<i>List of Tables</i>	<i>xxx</i>
1 Chapter 1: Introduction	1
1.1 Introduction	3
1.2 Research Aims and Objectives	5
1.3 Research Hypothesis	7
1.4 Research Scope	7
1.5 Contribution of the Thesis	9
1.6 Structure of the Thesis	10
2 Chapter 2: Cloud Computing in Healthcare	13
2.1 Introduction	15
2.2 Cloud Computing in Healthcare	15
2.3 Examples of Cloud Computing in Healthcare	18
2.4 Strategic Importance of Cloud Computing in Healthcare	21
2.4.1 Benefits of Cloud Computing	21
2.4.2 SWOT Analysis for Using Cloud Computing in Healthcare Sector	23
2.5 Risks of using Cloud Computing in Healthcare	26
2.5.1 Management Risks.....	26
2.5.2 Technological Risks.....	28
2.5.3 Legal Risks	31
2.5.4 Security Risks	33
2.5.5 Summary of Risks.....	34
2.6 Conclusion	41
3 Chapter 3: Understanding the Perception of Risk Using Cloud Computing in Healthcare in Oman	43

3.1	Introduction	45
3.2	Healthcare in Oman	45
3.3	Research Methodology	48
3.3.1.	Research Problem:	49
3.3.2.	Research Aim:	49
3.3.3.	Research Question	49
3.3.4.	Data Collection:	49
3.3.5.	Research Validation:	49
3.4	Data Collection: Qualitative Semi-structured Interviews	50
3.5	Hypothetical Case Study	52
3.5.1	Findings	53
3.5.1.1	Human Factors	53
3.5.1.2	Technological Factors	55
3.5.1.3	Organisational Factors	58
3.5.1.4	Environmental Factors	59
3.6	Data Collection: Quantitative - Creating Questionnaires	63
3.7	Data Analysis and Results	67
3.7.1	Reliability and Validity	67
3.7.2	Radar Chart	72
3.7.2.1	Construct for Radar Chart	72
3.7.2.2	Analysis of Data Security Construct	74
3.7.2.3	Analysis of Confidentiality, Integrity, Availability Construct	75
3.7.2.4	Analysis of Complex and Cost Construct	76
3.7.2.5	Analysis of Privacy Construct	77
3.7.2.6	Analysis of Human Construct	78
3.7.2.7	Analysis of Compatible Construct	79
3.7.2.8	Analysis of Relative Advantage Construct (Healthcare Professional)	80
3.7.2.9	Analysis of Top Management Support Construct (Healthcare Professional)	81
3.7.2.10	Analysis of Adequate Resource Construct (Healthcare Professional)	82
3.7.2.11	Analysis of Benefit Construct (Healthcare Professional)	83
3.7.2.12	Analysis of Environmental Construct (Healthcare Professional)	84
3.8	Research Validation	85
3.9	Reflection on Results	87
3.10	Conclusion	90
4	Chapter 4: Managing Information Security in Healthcare	93
4.1	Introduction	95
4.2	Corporate Governance of Information Technology (ISO 38500)	96

4.3	Risk Management (ISO 31000)	98
4.4	Managing Information Security Risk (ISO 27000)	101
4.5	Information Security Risk Management (ISO 27005)	104
4.6	Analysis of the Different ISO Standards and Methodologies	108
4.6.1	ISO 38500 IT Governance	108
4.6.2	Organisational Risk Management Methods.....	111
4.6.3	Methods of Managing Information Security Risk	117
4.7	Managing Information Security Risk in Healthcare	124
4.7.1	Risk Register.....	125
4.7.2	Operationally Critical Threat and Vulnerability Evaluation (OCTAVE)	129
4.7.3	Failure Modes and Effect Analysis (FMEA).....	130
4.8	Comparison of Risk Management Tools in Healthcare	131
4.9	Risk Register Benefits and Limitations	135
4.10	Information Security	136
4.11	Business Process Modelling (BPM)	139
4.12	Examples of Using BPM to Model Security	140
4.13	Reflection	143
4.14	Conclusion	145
5	<i>Chapter 5: Methodology Framework</i>	147
5.1	Introduction	149
5.2	Using RMIAS to Develop a Generic Reference Risk Register Table .	150
5.3	Managing Security Risk-Business Process Model (MSR-BPM)	
	Approach	166
5.3.1	Establish Context	171
5.3.2	Identify Risk	171
5.3.3	Generate Risk Register	172
5.3.4	Risk Evaluation.....	173
5.3.5	Define Security Goal	174
5.3.6	Identify Countermeasure	175
5.3.7	Update Risk Register with Traceability.....	176
5.4	Anticipated Benefit of Combining Risk Register with BPM	177
5.5	Reflection	180
5.6	Conclusion	182
6	<i>Chapter 6: Application of The MSR-BPM Methodology</i>	185
6.1	Introduction	187

6.2	Hypothetical Case Study Scenario	187
6.2.1	Establishing the Context.....	192
6.2.1.1	Author’s Approach.....	192
6.2.1.2	Consideration for Stakeholder Team of MSR-BPM.....	193
6.2.2	Identify Risk.....	194
6.2.2.1	Author’s Approach.....	194
6.2.2.2	Consideration for Stakeholder Team of MSR-BPM.....	196
6.2.3	Generate Risk Register.....	196
6.2.3.1	Author’s Approach.....	196
6.2.3.2	Consideration for Stakeholder Team of MSR-BPM.....	197
6.2.4	Evaluate Risk.....	197
6.2.4.1	Author’s Approach.....	197
6.2.4.2	Consideration for Stakeholder Team of MSR-BPM.....	198
6.2.5	Define Security Goals.....	199
6.2.5.1	Author’s Approach.....	199
6.2.5.2	Consideration for Stakeholder Team of MSR-BPM.....	201
6.2.6	Identify Countermeasure.....	202
6.2.6.1	Author’s Approach.....	202
6.2.6.2	Consideration for Stakeholder Team of MSR-BPM.....	204
6.2.7	Updated Risk Register with Traceability.....	205
6.2.7.1	Author’s Approach.....	205
6.2.7.2	Considerations for Stakeholder Team of MSR-BPM.....	205
6.3	Current situation	209
6.4	Cloud Computing Solution	214
6.5	Reflection	232
6.6	Conclusion	237
7	Chapter 7: Framework Evaluation	239
7.1	Introduction	241
7.2	Comparing MSR-BPM with Other Research Work	241
7.3	Breast Cancer Treatment Scenario	243
7.4	Apply MSR-BPM Approach in Integrated Care Pathway	245
7.4.1	Establishing the Context.....	245
7.4.2	Identify Security Risks.....	246
7.4.3	Generate Risk Register.....	247
7.4.4	Evaluate Risk.....	247
7.4.5	Define Security Goal.....	250
7.4.6	Identify Countermeasure.....	252
7.4.7	Updated Risk Register Table with Traceability.....	253
7.5	Evaluation Methodology	255
7.6	Evaluation Methodology for MSR-BPM	256
7.6.1	ISO 27005 Risk Management Processes.....	257

7.6.2	Design of the Survey Questions	258
7.6.3	Pilot Study of the Experiment.....	263
7.6.4	Record Video of the Experiments and Prepare URL.....	264
7.6.5	Contact the Experts.....	264
7.6.6	Analysis of Survey Feedback	265
7.6.6.1	Participant Profile from UK	265
7.6.6.2	Participant Feedback on Questions 14 to 25	265
7.6.6.3	Participant Feedback about MSR-BPM Q26 to Q29	270
7.6.6.4	Evaluating MSR-BPM with Stakeholder from Oman.....	277
7.6.7	Evaluate MSR-BPM in ISO 27005 Process	279
7.6.7.1	Advantages of MSR-BPM.....	279
7.6.7.2	Limitations.....	281
7.6.7.3	Evaluation of the Approach to Determine Risks.....	282
7.6.7.4	Future Work	287
7.7	Conclusion.....	289
8	Chapter 8: Conclusion.....	293
8.1	Introduction	295
8.2	Achievements of the Research Objectives.....	295
8.2.1	Research Objective One	295
8.2.2	Research Objective Two.....	296
8.2.3	Research Objective Three.....	297
8.2.4	Research Objective Four.....	299
8.2.5	Research Objective Five	301
8.2.6	Research Objective Six.....	303
8.3	Originality and Significance of Research Contribution	306
	References	313
	Appendixes.....	330
	Appendix A: Interview Questions.....	332
	A.1: Interview Questions to Managers to Migrate Healthcare Services to Cloud.....	332
	A.2 Glossary Terms for Interview Questions	335
	A.3 Interview Transcript with CC01.....	338
	A.4 Interview Transcript with CC02.....	342
	A.5 Interview Transcript with CC03.....	345
	A.6 Interview Transcript with CC04.....	353
	A.7 Interview Transcript with CC05.....	356
	A.8 Interview Transcript with CC06.....	359
	A.9 Interview Transcript with CC07.....	369

A.10 Interview Transcript with Undersecretary for Planning Affairs.....	375
Appendix B: Questionnaires.....	378
B.1 Questionnaire Justification.....	378
B.2 Public Questionnaire.....	386
B.3 Healthcare Professionals Questionnaire.....	396
B.4 Authorisation Letter from SQU.....	409
B.5: Demographic Data of Respondent.....	410
B.6: Rotated Component Matrixa for Public and Healthcare Professional.....	412
B.7: Rotated Component Matrixa for Healthcare Professional.....	414
B.8: Radar Charts Tables.....	415
B.9 : Healthcare Professional.....	419
Appendix C: Generic Reference Risk Register Table.....	422
Appendix D: Hypothetical Scenario BPM and Risk Register Table.....	458
Appendix D 1: Generic Health Centre Workflow.....	458
Appendix D .2 First Modelling Attempt.....	459
Appendix D 2.1 Risk Register Table For First Modelling.....	460
Appendix D.3 BPM for Hospital Process.....	464
Appendix D 3.1 Oman Hospital Risk Register Table.....	465
Appendix D 4: Patient BPM.....	469
Appendix D 4.1 Patient Process Risk Register Table.....	470
Appendix E: Integrated Care Pathway.....	472
E.1 Full Set of BPM for Integrated Care Pathway.....	472
E.2 Patient Pathway in GP with Countermeasures.....	476
E.3 Risk Register for Patient pathway in GP Referral.....	477
E.4 Patient Pathway in Hospital 1 with Countermeasures.....	482
E.5 Risk Register for Patient Pathway in Hospital 1.....	483
E.6 Patient Pathway in Hospital 2 with Countermeasures.....	489
E.7 Risk Register for Patient Pathway in Hospital 2.....	490
E.8 Patient Pathway in Hospital 3 with Countermeasures.....	492
E.9 Risk Register for Patient Pathway in Hospital 3.....	493
Appendix F: Evaluation Methodology.....	495
F.1 Participation in a Research Evaluation.....	495
F.2 Survey Questions.....	496

F.3 Participant Profile Part 1	503
F.4 Participant Profile Part 2	507
F.5 Participant Feedback for Q14 to Q25	510
F.6 Participant Feedback for Q26- Q30	512
Feedback from Participant 1	512
Feedback from Participant 2	514
Feedback from Participant 3	515
Feedback from Participant 4	516
Feedback from Participant 5	517
Feedback from participant 6	518
Feedback from Participant 7	519
Feedback from Participant 8	520
Feedback from participant 9	521
Feedback from Participant 10	522
Feedback from participant 11	523
Feedback from Participant 12	525

List of Figures

Figure 2-1 NIST Definition of Cloud Computing	16
Figure 2-2 A Framework for EHR Based on Mobile Cloud Computing and Big Data Analytics	17
Figure 2-3 Pilot e-Health System at Chelsea and Westminster Hospital (London)...	19
Figure 2-4 Heath-CPS Architecture	20
Figure 3-1 Research Methodology Stages	48
Figure 3-2 Data Security	74
Figure 3-3 Confidentiality, Integrity and Availability	76
Figure 3-4 Complex & Cost.....	77
Figure 3-5 Privacy.....	78
Figure 3-6 Human	79
Figure 3-7 Compatible	80
Figure 3-8 Relative Advantage	81
Figure 3-9 Top Management Support.....	82
Figure 3-10 Adequate Resource.....	83
Figure 3-11 Benefit	84
Figure 3-12 Environmental	85
Figure 4-1 Model for Governance of IT	97
Figure 4-2 Risk Management Perspectives.....	100
Figure 4-3 Illustration of Information Security Risk Management Process	105
Figure 4-4 Risk Treatment Option	107
Figure 4-5 COBIT 5 For Risk of Other Standards and Framework.....	109
Figure 4-6 COBIT 5 for risk	113
Figure 5-1 The Reference Model of Information Assurance & Security (RMIA)S	152
Figure 5-2 Information Security Risk Management ISMS Processes	154
Figure 5-3 MSR- BPM Process	170
Figure 5-4 Risks Types	172
Figure 5-5 Countermeasure Shape and Name.....	175
Figure 6-1 Generic Workflow in Oman Hospital	189
Figure- 6-2 Patient BPM Diagram	191
Figure 6-3 Patient's Hospital BPM.....	193
Figure 6-4 Identify Risk in patient's Hospital Process	195
Figure 6-5 Evaluate Risk Level in patient's Hospital Process.....	198
Figure 6-6 Identify Security Goals in patient's Hospital Process	201
Figure 6-7 Patient's Hospital BPM Updated with Risk Countermeasure.....	204
Figure 6-8 Current Situation in Oman Hospital.....	210
Figure 6-9 Patient Process with Potential Risks	211
Figure 6-10 Oman Cloud	215
Figure 6-11 Germany Cloud	216
Figure 6-12 Patient pathway within OH for cloud permission	218

Figure 6-13 Patient Treatment Pathway in Germany.....	219
Figure 6-14 Cloud Computing BPM with Risks.....	224
Figure 6-15 Enterprise Architecture	235
Figure 6-16 Different Dimensions for Managing Risks	236
Figure 7-1 Sample of Doctor Process in GP Surgery	246
Figure 7-2 Identify Security Risks in Doctor Process.....	246
Figure 7-3 Risk Evaluation	248
Figure 7-4 Evaluate Security Risks in Doctor Process	250
Figure 7-5 Countermeasure Security Risks Identified in Doctor Process	252
Figure 7-6 ISO27005 Information Security Risk Management Process.....	256
Figure 7-7 BPM of Evaluation Methodology	257
Figure 7-8 Sample of the Survey Questions Design	259
Figure 7-9 Summary of Stage 1 Analysis	266
Figure 7-10 Summary of Stage 2 Analysis	267
Figure 7-11 Summary of Stage 3 Analysis	267
Figure 7-12 Summary of Stage 4 Analysis	268
Figure 7-13 Summary of Stage 5 Analysis	269
Figure 7-14 Summary of Stage 6 Analysis	270

List of Tables

Table 2-1 Examples of Key Benefits in a Cloud-based Healthcare System.....	23
Table 2-3 SWOT Analysis for Cloud Computing in the Healthcare Sector.....	25
Table-2-3 Summary of Risks	40
Table 3-1 Justification of the Interview Questions	51
Table 3-2 Demographics of Interviewees	52
Table 3-3 Summary of Interviews Findings	62
Table 3-4 Questionnaire Structure	64
Table 3-5 Factor loading and Cronbach’s Alpha for Public and Healthcare Professionals	70
Table 3-6 Factor loading and Cronbach’s Alpha for Healthcare Professionals.....	71
Table 3-7 Sample of Response Percentage for Data Security Construct.....	73
Table 4-1 Alignment of ISMS and Information Security Risk Management Process	106
Table 4-2 Governance Framework	110
Table 4-3 Organisational Risk	116
Table 4-4 IT Security System Risk	123
Table 4-5 Comparison Between Managing Information Security Risk Techniques in Healthcare	134
Table 4-6 Summary of Various Information Security Definitions	136
Table 5-1 Sample of Risk Evaluation to Risk Register	155
Table 5-2 Sample Row of Updated Risk Register	158
Table 5-3 Sample of Management Risk.....	160
Table 5-4 Sample of Security Risk	161
Table 5-5 Sample of Technical Risk.....	162
Table 5-6 Sample of Legal Risk	163
Table 5-7 Summary of Different Level Risks.....	165
Table 5-8 Comparison Table between BPMN, Secure*BPMN and MSR-BPM....	168
Table 5-9 Sample of Risk Register	172
Table 5-10 Information Classification Scheme	174
Table 5-11 Updated Risk Register with Security Goal.....	175
Table 5-12 Benefits of Using Risk Register with BPM.....	179
Table 6-1 Oman Hospital Risk Register	196
Table 6-2 Oman Hospital Updated Risk Register with Evaluated Risk	197
Table 6-3 Oman Hospital Updated Risk Register with Security Goals.....	200
Table 6-4 Patient’s Hospital Updated Risk Register with Countermeasures.....	203
Table 6-5 Oman Hospital Updated Risk Register with Traceability	208
Table 6-6 Patient Process Risk Register Table	213
Table 6-7 Cloud Computing Risk Register Table.....	231
Table 7-1 Sample of Doctor Process Risk Register	247

Table 7-2 Sample of Doctor Process Risk Register-Evaluation 249

Table 7-3 Updated Risk Register with Security Goals 251

Table 7-4 Sample GP Referral- Doctor Process Risk Register Table..... 254

Table 7-5 Justification of Survey Questions to Evaluate MSR-BPM Approach..... 263

Table 7-6 Summary of Evaluator Background. 265

1 Chapter 1: Introduction

1.1 Introduction

Information security is an issue of growing importance in recent years and is discussed on the agenda of governing boards and directors (Subramaniam et al., 2011; Rasid et al., 2017). It is viewed as a critical aspect of an organisation's information security risk management where timely identification, assessment and management of risks are linked with the achievement of its goals and objectives (Subramaniam et al., 2011). As organisations adopt new technologies, they need to update risk management processes to mitigate the identified risk with minimum loss.

Healthcare systems are trying to improve their services and enhance collaboration among medical institutions and hospitals, such as by sharing medical imaging and data. Also, the adoption of digital patient records, increased regulation, provider unification and the increasing need for information exchange between patient, providers and payers, all point towards the need for better information security. Patient data can be easily stored in virtual archives that are accessible by different healthcare providers; thus, facilitating data-sharing and significantly reducing local storage requirements. A potential solution can be through utilising cloud-computing services as a technology mechanism that enhances the communication between different locations (Ren et al., 2017). However, this solution may raise different types of risks. Patient data security and privacy issues arise from the use of cloud systems for confidential personal data.

Using cloud computing in healthcare can bring many benefits to healthcare providers and patients. The current healthcare system in Oman has short-comings in many areas: (i) it does not support a patient-centric approach, (ii) it does not allow a patient to access his/her medical records online and, (iii) it does not facilitate a patient in seeking treatment from other healthcare providers (i.e. does not enable information-sharing between healthcare providers). Adopting cloud computing can provide a potential solution to address all these limitations.

However, healthcare providers in Oman are hesitant to use cloud computing in healthcare services. Security risks in using cloud computing in the delivery of healthcare services is the main barrier. One of the objectives of this research is to investigate how Omani stakeholders perceive cloud computing. Also, it seeks to understand the challenges and key risk factors that affect cloud computing adoption for healthcare provision in the public and private sector. There are a broad range of different types of risks, such as management, technical, legal and security risks. The perception of risks identified include Data Security, Confidentiality, Integrity and Availability as well as Privacy, Human, Complex and Cost risks within the Omani context.

Risk Management Standards provide general guidelines to help organisations address risks and promote mitigation solutions. Also, those standards provide examples to help organisations comply with its rules. This research focuses on; the business context through ISO/IEC 38500 for Corporate Governance of Information Technology, Risk Management, (ISO 31000), Information Security Management Systems (ISO 27000) and Information Security Risk Management (ISO 27005). Risk management standards provide a wide range of guidelines with useful examples for addressing risks . However, they are high-level generic guidelines, which may represent a challenge for organisations to implement in their specific domains. In addition to the risk management standards, there are various approaches to manage risks, such as Risk Register (RR), Operational Critical Threat and Vulnerability Evaluation (OCTAVE), and Failure Modes and Effect Analysis (FMEA). In the healthcare system, Risk Registers are widely used to prioritise and manage risks but there are limitations, such as not visualising the risk location for stakeholders. Therefore, there is a need for effective risk management approaches to address risks in moving to new technology, such as cloud computing, in the current healthcare system.

This research focuses on information security risk management; stakeholder perceptions in Oman identified Data Security, Confidentiality, Integrity and Availability are the major concerns of this research. It is, therefore, necessary to

consider information security management standards and approaches to address these concerns.

This research presents a methodology, Managing Information Security-Business Process Modelling (MSR-BPM), which links the use of Risk Register with Business Process Models to address risks associated with healthcare. A risk register documents the assessment of risk with appropriate countermeasures. BPM visualises the risk activities, security goals and countermeasures in the process models to promote a shared understanding of risks to decision makers and stakeholders. Also, MSR-BPM is enriched with stakeholder perceptions of risks. The approach has been evaluated by a range of experts using Integrated Care Pathway (ICP) scenario to test its effectiveness in the healthcare industry.

1.2 Research Aims and Objectives

Healthcare information systems use a variety of applications and infrastructures to improve the quality of healthcare services. Cloud computing enables location-independent access to data and plays a significant role in a “linked-up” healthcare environment. Having cloud computing not only improves the availability of patient medical records, but it also means having the right process in place to enhance the healthcare information system with advanced technological services to improve the patient treatment, avoid multiple tests and link the collaboration and communication among healthcare institutions in different locations. However, data security represents the main barrier in adopting cloud computing as a service (Masrom and Rahimli, 2015). Hence, the healthcare sector needs an effective risk management framework to reduce risk to an acceptable level. In addition, there is an issue with approaches to enhance communication within different locations. Therefore, the aim of this research is to:

Develop a methodology to manage risks which improves the communication of information security risk in healthcare processes

The research objectives are:

1. To survey the literature to understand the benefits, challenges and risks associated with utilising cloud computing in healthcare and how relevant it is to the healthcare context in Oman.
2. To understand stakeholders' perceptions of risks in utilising cloud computing in the delivery of healthcare services.
3. To understand the framework and techniques used to manage risks and business process modelling to visualise risks.
4. To develop an approach to address the stages of Information security risk management (ISO 27005) process and determine how to combine both the risk register and business process models to communicate the information security risks .
5. To identify healthcare scenarios to explain the need for migrating healthcare services to cloud computing and applying it to the identified scenarios.
6. To evaluate the proposed approach by experts across the field of risk management, business process management and healthcare, through an Integrated Care Pathway scenario.

To achieve these aims and objectives, it is necessary to study cloud computing benefits, as well as the challenges and risks of using cloud computing as services in healthcare. In addition, it will be necessary to study risk management standards, and especially Information Security Management Systems (ISO 27000) and Information Security Risk Management (ISO 27005).

1.3 Research Hypothesis

Information security management represents an important element in any organisation. Healthcare information security management widely uses risk register to document and prioritise risk. Risk register provides an assessment of risks with appropriate countermeasures. However, it has limitations as it does not visualise the risk location for stakeholders. Thus, an effective information security risk management approach is necessary to provide a holistic view of any anticipated risks and visualize risks in the process models in order to promote a shared understanding of risks among decision makers and stakeholders. Therefore, the research hypothesis is as follows:

The communication of Information Security Risk in Healthcare processes can be improved by combining risk register and business process modelling to visualise risks in healthcare process and achieve a shared understanding of these risks for stakeholders

1.4 Research Scope

In many developing countries, there is the need to have medical care and resources, such as professional doctors and nurses, financial support and community care (Alagoz et al., 2010). However, there are security concerns and so healthcare providers need to search for advanced and economical solutions to solve this problem. Adopting cloud computing is likely to provide benefits in addressing these problems but there are anticipated risks in using cloud computing as a service. These risks require an effective approach to address them.

This research focuses on the business context through ISO/IEC 38500 for Corporate Governance of Information Technology, Risk Management (ISO 31000), Information Security Management Systems (ISO 27000) and Information Security Risk Management (ISO 27005). It observes each standard's usefulness, methods and

theoretical background. Also, the research observes various methods and techniques used within information security risk management as a tool to reduce risk to the lowest level. Risk Register (RR), Operational Critical Threat and Vulnerability Evaluation (OCTAVE) and Failure Modes and Effect Analysis (FMEA) are widely used in the healthcare system, but there are limitations in their use. Therefore, the focus of this research is to find an appropriate approach for an effective communication of information security risk within healthcare systems; thus, enhancing communication.

This research centres on information security risks to address the potential risks in the current systems and cloud computing. It will be suggested that combining Risks Register with Business Process Modelling can assist with traceability of the risks. The ISO 27005 Information Security Risk Management Process was followed at each stage in detail, which helped to structure the thought process about the security risks and ensure that each activity in the process had been addressed. ISO 27005 was chosen as it is an international information security standard which is widely used to manage risks. The MSR-BPM approach highlights the importance of enhancing the use of a risk register with business process modelling to provide a more effective way to communicate risks. However, there are limitations concerning the use of Risk Register and business process as the list of risks tends to grow leading the business process modelling to have overcrowded symbols of risks. Therefore, there is a need for a multidisciplinary team to have an open discussion regarding which level they need to address the risks in certain situations. The link between the growing list of risks and BPM will be addressed in Chapter 6 in detail.

The main contribution of this research is its attempt to develop MSR-BPM methodology to identify and manage security risks. The approach links the use of risk register with BPM rather than using a risk register only. The MSR-BPM approach is validated through an integrated care pathway for breast cancer treatment to verify its usefulness and significance in a realistic scenario. Experts from risk management, business process modelling and healthcare were involved in the validation process.

1.5 Contribution of the Thesis

This inter-disciplinary research contributes to the domain of Information Security Risk Management and Health Informatics by:

1. Providing a comprehensive study about the perception of different types of risks (Security, Management, Technical, Legal, Privacy and Other types of risks) in adopting cloud computing as a service in the delivery of healthcare services within the Omani context.
2. Creating a comprehensive Generic Reference Risk Register to address risks of migrating cloud computing in healthcare. The Reference Model of Information Assurance & Security (RMIAAS) (Cherdantseva, 2014) was used as a basis to include risk name, description, impact, likelihood, risk level, security goals, and countermeasure. Traceability was added to show risk location. Also, the Generic Reference Risk Register table includes various types of risks, such as security, management, technical, legal and cloud computing risks. The relevance of each of the identified risks to the Omani context is also provided.
3. Providing an extension to Secure*BPMN (Cherdantseva, 2014) by adding risk representation. It is important to visualize the risks in BPM diagram for stakeholders and decision makers.
4. The main contribution of this research relates to creating a methodology, Manage Security Risk-Business Process Modelling (MSR-BPM), to visualise risks in a healthcare process and promote a shared understanding of the risks for stakeholders. It follows Information Security Risk Management (ISO 27005) processes to improve the communication of information security risk management by combining risk register and business process modelling. A risk register documents the assessment of risk with appropriate countermeasures. BPM visualises the risk activities, security goals and countermeasures in the process models to promote a shared understanding of risks to decision makers and stakeholders.

These contributions are discussed and justified in the conclusion chapter (section 8.3).

In addition, the author has participated in several conferences, notably:

- Aseela Al Harthi, Wendy Ivins, Omer Rana (2015) 'Perception of security using cloud computing in the delivery of healthcare services in Oman and Saudi Arabia'. *1st International Saudi Health Informatics Conference Emerging Trends and Technologies in Health Care*. Riyadh, Saudi Arabia.
- Aseela Al Harthi, Wendy Ivins, Omer Rana (2017) 'Perception of security using cloud computing in the delivery of healthcare services in Oman'. *7th Conference Pharmacy Care: "Towards Professional Excellence in Pharmacy"* Al Bustan Palace Hotel, Muscat. Oman.
- Aseela Al Harthi, Wendy Ivins, Omer Rana (2017) 'Perception of security using cloud computing in the delivery of healthcare services in Oman.' *Speaking of Science: "An Interdisciplinary Conference for Natural and Applied Scientists"* 4th May, 2017, Cardiff, UK.

1.6 Structure of the Thesis

The remaining chapters will outline the thesis structure.

Chapter 2: provides background information about cloud computing in healthcare. It highlights the general definition of cloud computing and how it can be customised for the healthcare industry. It discusses various examples related to adopting cloud computing in healthcare. In addition, it presents the strategic importance of adopting cloud computing as a service through listing its benefits and performing a SWOT analysis. Also, anticipated risks are discussed in regard to management, technical, legal and security risks. In addition, the importance and relevance of each risk were explored in detail.

Chapter 3: this chapter explores the stakeholders' perception of risk in Healthcare Systems in Oman. In addition, it presents the mixed research methods (qualitative and quantitative) that were used to collect data. A preliminary interview with stakeholders was performed and two sets of questionnaires were issued for public and healthcare professionals in order to understand their perception of adopting cloud computing as

a service in healthcare. Data analysis was performed by using an advanced statistical method (SPSS). Exploratory Factor Analysis (EFA) was used to investigate the interrelationships between items, reduce their number and form them into constructs. In addition, each statement was carefully analysed to identify stakeholder perception. Radar Charts were used to visualize the public and healthcare professionals' perception and an analysis was performed regarding whether they agreed or disagreed. In addition, research validation was conducted through an interview with H. Dr. Ali Talib Al Hinai, Undersecretary for Planning Affairs in Ministry of Health. The outcome will emphasise the need to find an effective risk assessment methodology to overcome various risks identified. The findings are reflected upon and recommendations and suggestions are made for the Omani government.

Chapter 4: presents the management of information security risks as the research problem. It discusses the business context through ISO/IEC 38500 for Corporate Governance of Information Technology, Risk Management standard (ISO 31000) as it is widely used in managing risks. In addition, Managing Information Security (ISO 27000) and Information Security Risk Management (ISO 27005) is discussed to understand the mechanism in managing information security risks. A critical analysis of the tools and techniques for each standard is presented. Tools and techniques for managing risks in healthcare are explored. A review of Information Security is presented as a major concern to address in this research. The role of process modelling prospected in risk management framework is considered.

Business Process Modeling (BPM) is discussed as a widely used modelling technique, especially in healthcare, and is used to model information security in healthcare processes.

Chapter 5: this chapter introduces an approach for managing information security risks. It includes three contributions of this research. Firstly, it discusses the creation of a comprehensive Generic Reference Risk Register Table. In addition, it explains the expansion of Secure*BPMN (Cherdantseva, 2014) by adding risk representation

to it. Thirdly, it discusses the creation of an approach, Managing Security Risk-Business Process Modelling (MSR-BPM), to visualise risks in a healthcare process and promote a shared understanding of the risks for stakeholders. A reflection is provided based on the challenges and difficulties faced while developing the MSR-BPM approach.

Chapter 6: introduces the application of MSR-BPM approach through a hypothetical case study scenario which was used during the preliminary interview in Chapter 3. It utilises MSR-BPM approach as a way to manage risks based on ISO 27005 process in two ways: this research approach and the stakeholders' consideration. Also, it presents the choice of communication mechanism by looking at a current situation with potential risk and cloud computing as a solution to enhance the collaboration and communication between an Omani hospital and German hospital. It addresses the anticipated risks with cloud computing based on the approach used in this research.

Chapter 7: presents an evaluation of MSR-BPM approach through specific research undertaken within the Computer Science and Informatics at Cardiff University which uses Integrated Care Pathway (ICP) for breast cancer treatment. It has many potential risks, and the process involves multiple locations as well as stakeholders. Information Security Risk Management (ISO 27005) processes and a number of quality criteria are adopted to design a set of survey questions for experts who have experience in one or more of Risk Management, Business Process Modelling and Healthcare. Reflections are offered on the MSR-BPM approach based on ISO 27005 processes. Advantages, limitations and future work which could be carried out based on this research are discussed.

Chapter 8: summarizes the key aspects of the research and assesses the achievements against the aims and objectives. It provides a reflective analysis based on the extent to which the research hypothesis was achieved.

2 Chapter 2: Cloud Computing in Healthcare

2.1 Introduction

This chapter provides a background of cloud computing in healthcare. It highlights the cloud computing definition in general and how it can be defined within the context of the healthcare domain. It presents various examples of using cloud computing in healthcare. In addition, it illustrates the strategic importance of adopting cloud computing as a service by highlighting its benefits and performing a SWOT analysis. Then, it examines potential risks and threats of providing cloud computing as a service in the delivery of healthcare services, such as management, technical, legal and security risks. These potential risks were summarised in risk register. The risk register was expanded to highlight the relevance and importance of identified risks according to the Omani context.

2.2 Cloud Computing in Healthcare

This thesis will consider the problem of using cloud computing as a service in the healthcare industry in Oman, which is discussed further in Chapter 3. Therefore, a brief overview of cloud computing is needed to clarify its role. The often cited definition from the National Institute of Standards and Technology (NIST), by Mell and Grance (2011) explains that, *“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”*.

Cloud computing in healthcare can be defined as an application-oriented and services-based infrastructure where Health-IT resources are pooled, allowing services to be widely deployed or rapidly shared in response to changing healthcare business and regulatory requirements (e.g. networks, servers, storage, applications and services) (Liu & Park 2013). [Figure 2-1](#) represents the NIST definition of cloud computing. It focuses on computing resources that can be accessed from anywhere and at any time

and can be monitored online (Ren et al., 2017). It pinpoints five characteristics of cloud computing, three service models and four deployment methods.

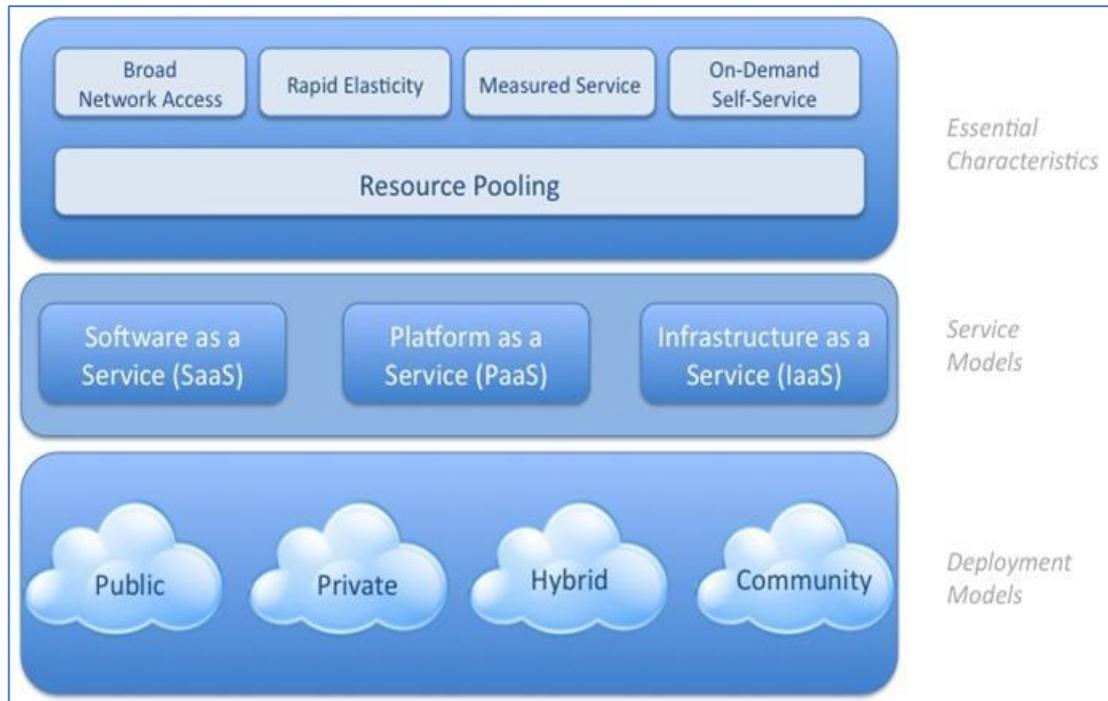


Figure 2-1 NIST Definition of Cloud Computing

The NIST definition of cloud computing is relevant to the healthcare domain in many areas. The essential characteristics of cloud computing can be customized to healthcare to provide rapid provisioning and interconnectivity of electronic resources (Shini et al., 2012; Liu & Park, 2013; Uta, 2014; Devadass et al., 2017), enhanced data availability (Shini et al., 2012; Ahuja, 2012; Mxoli et al., 2014; Masrom & Rahimli, 2014; Devadass et al., 2017), improved patient quality of service and reduced overall healthcare costs (Shini et al., 2012; Ahuja, 2012; Mxoli et al., 2014; Masrom & Rahimli, 2014). Table 2.1 discusses further benefits in detail.

In addition, a study by Youssef (2014) proposed a framework for secure Health Information Systems (HISs) based on big data analytics in mobile cloud computing environment. As can be seen in [Figure 2-2](#), the framework provides a high level of integration, interoperability, and sharing of EHRs among healthcare providers, patients and practitioners. The cloud permits fast Internet access, sharing, and provision of EHRs by authenticated users. Big data analytics helps analyse patient data

to provide the right intervention to the right patient at the right time. The proposed framework applies a set of security constraints and access control that guarantee integrity, confidentiality, and privacy of medical data. The ultimate goal of the proposed framework is to introduce a new generation of HISs that are able to provide healthcare services of high quality and low cost to patients using this combination of big data analytics, cloud computing and mobile computing technologies (Youssef, 2014).

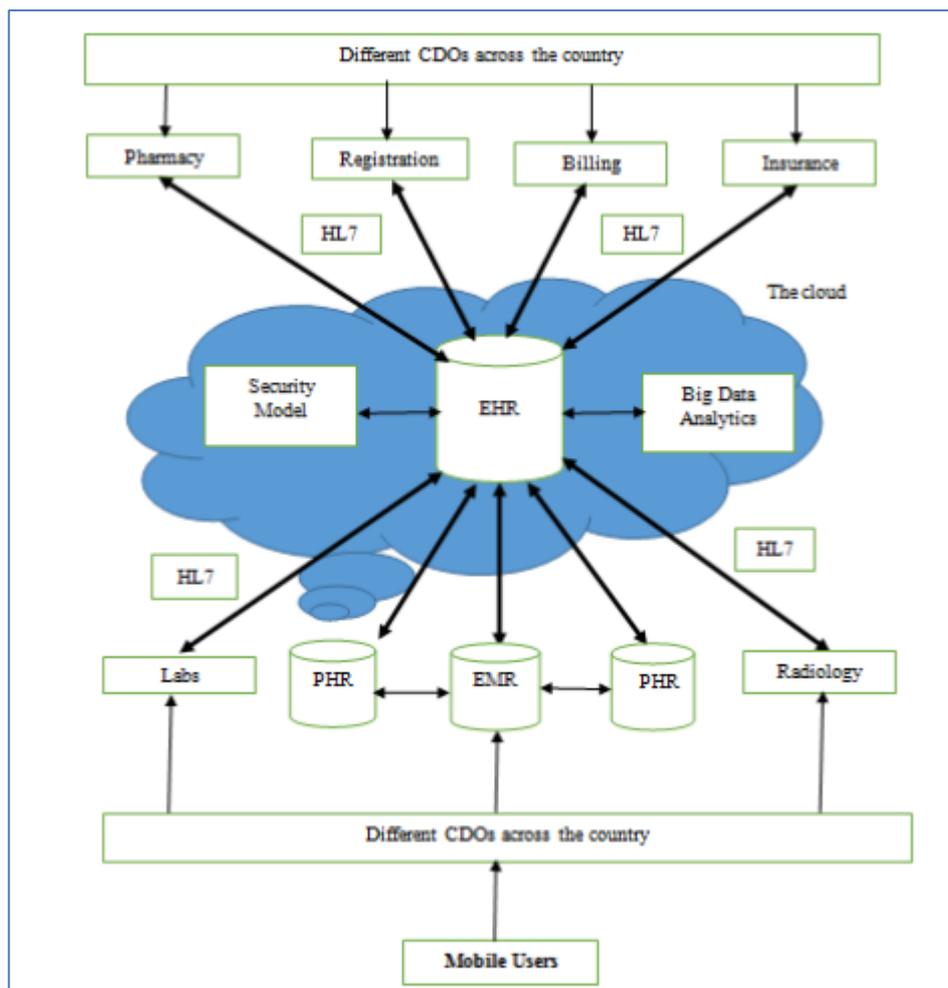


Figure 2-2 A Framework for EHR Based on Mobile Cloud Computing and Big Data Analytics
Source: (Youssef, 2014)

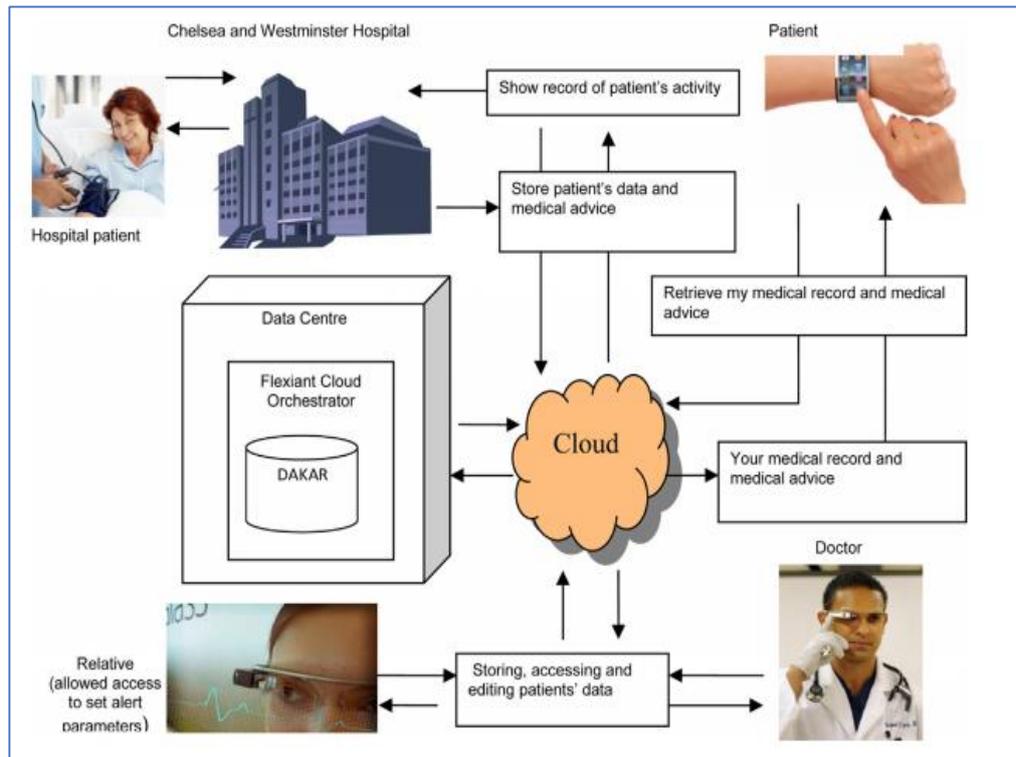
Of particular interest was the use of cloud computing in healthcare in Oman. Regarding service models, the Ministry of Health (MoH) in Oman uses Infrastructure as a service to host the ministry website. In addition, it uses Software as a Service (SaaS) in Al Shifa project to allow patients to book/cancel an appointment with a

healthcare establishment as long as they are registered with online services. According to Zhang et al. (2017), using Cloud Service Models in healthcare will solve the big data and storage problem that currently represents a challenge in terms of handling and processing. The technologies of cloud and big data can be used to enhance the performance of the healthcare system so that patients and practitioners can then enjoy various smart healthcare applications and services (Zhang et al., 2017).

Healthcare organisations can use deployment models such as Hybrid to use two or more cloud models to maintain the privacy of their data. The next section will discuss detailed examples regarding the use of cloud computing in healthcare domain.

2.3 Examples of Cloud Computing in Healthcare

The UK government is observing the use of cloud computing to allow its National Health Service (NHS) patients to access their Electronic Health Records (EHR). The NHS Future Forum was proposed in 2011 to advise the government on its health reforms. It was believed that there would be major financial benefits because fewer visits would be required to the medical centres and hospitals for consultation, and repeat prescriptions could be made online (Barrow, 2011). From 2009 to 2011, London's Chelsea and Westminster hospital piloted cloud-based healthcare (Sultan, 2014). They presented the first cloud prototype in Europe through an e-health project known as Data Capture and Auto Identification Reference (DACAR). It is a stack of software components and services that addresses common e-health application requirements, such as authorisation, data capture, data integrity and confidentiality. DACAR is cloud PaaS infrastructure (known as Flexiant Cloud Orchestrator) that provides tools to facilitate the development, integration and deployment of an e-health SaaS solution (Sultan, 2014). The system allows close and trusted circles of friends or relatives to access patients' data buckets (i.e., physical memory storage locations). If that data goes beyond trusted circles, the patient's family can be alerted, and this will allow them to go and check their physical conditions. With the arrival of wearable technology, such operations (as depicted in [Figure 2-3](#)) can be performed by wrist or eye-based devices such as Google Glass or Apple's iWatch (Sultan, 2015).



*Figure 2-3 Pilot e-Health System at Chelsea and Westminster Hospital (London)
Source: (Sultan, 2015)*

A study proposed a cyber-physical system for patient-centric healthcare applications and services, called Health-CPS, built on cloud and big data analytics technologies (Zhang et al., 2017). This system consists of a data collection layer with a unified standard, a data management layer for distributed storage and parallel computing, and a data-oriented service layer. The results of this study show that the technologies of cloud and big data can be used to enhance the performance of the healthcare system so that humans can then enjoy various smart healthcare applications and services (Zhang et al., 2017). The contributions of Health-CPS can be summarized as follows; 1) a unified data collection layer for the integration of public medical resources and personal health devices is presented; 2) a cloud-enabled and data-driven platform for the storage and analysis of multisource heterogeneous healthcare data is established; and 3) a healthcare application service cloud is designed, which provides a unified application programming interface (API) for the developers and a unified interface for the users (Zhang et al. 2017). [Figure 2-4](#) represents the Health-CPS architecture.

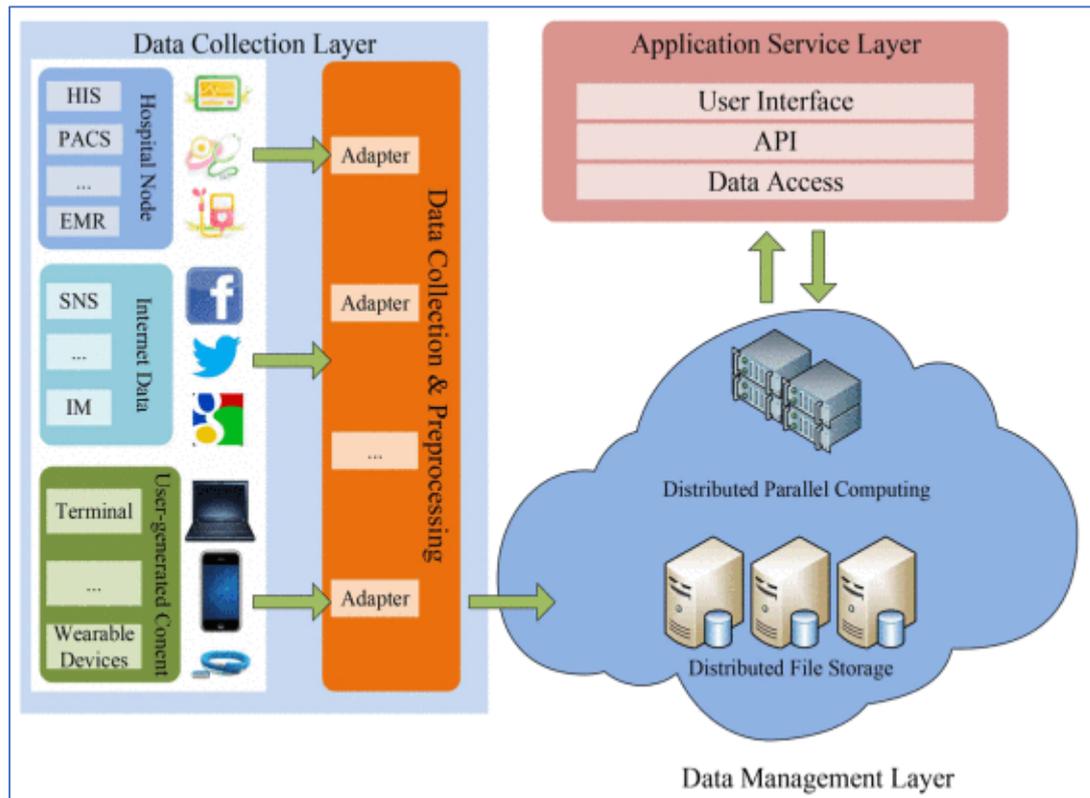


Figure 2-4 Heath-CPS Architecture
Source: (Zhang et al., 2017)

Using cloud computing technology has led to patient monitoring services that are dynamically scalable and universally accessible. One example is a suicide risk scouting prototype that functions by predicting mental states in the cloud environment (Alam et al., 2014). The system collects patient disease symptoms through a wireless body area network (WBAN) and then analyses the collected data in the healthcare cloud platform with the patient's history of disease, habits and genetics. Predicting mental states using some tiny sensors and cloud computing technology is a novel initiative to monitor patients presenting a suicide risk as well as those suffering from mental disorders (Alam et al., 2014).

A framework of an m-Health monitoring system (MHMS) based on a cloud computing platform (Cloud-MHMS) is proposed to support remote health monitoring, addressing health data integration and interoperability among various medical agencies (e.g. community hospitals and Class-A large hospitals). The multiple tenant data storage and access methods are designed to protect health data security and privacy (Xu et al., 2017). Similarly, Xu et al. (2017) linked the data model to represent health data and

connect them to open life data to supply background knowledge semantically to improve data interoperability (Xu et al., 2017).

Cloud computing in healthcare is suitable for managing medical data effectively, as well as being flexible and scalable in terms of access to e-Health services. Healthcare professionals will be able to attend to their patients from any location at any time. In addition, it will improve data quality operations, such as reducing the need to duplicate patient records stored in multiple databases (Devadass et al., 2017).

By considering the above examples of using cloud computing services in healthcare, it is hoped that this will provide an understanding of its usefulness as well as investigating the strategic importance of adopting cloud computing. The next section will discuss the strategic importance of cloud computing by exploring its benefits and performing a SWOT analysis to help decision-makers gain a clear picture of potential internal and external factors that may affect the adoption of cloud computing.

2.4 Strategic Importance of Cloud Computing in Healthcare

2.4.1 Benefits of Cloud Computing

Healthcare information systems use a variety of applications and infrastructures to improve the quality of healthcare services and cloud computing enables location-independent access to data and plays a significant role in a “linked-up” healthcare environment. Improving the availability of patient medical records is the primary objective; however, this must be in the context of particular security constraints. Assunção et al. (2015) provided a vision that cloud computing would become the fifth utility, which will provide the essential computing services for daily use. Cloud computing in healthcare can be defined as an application-oriented and services-based infrastructure, where Health-IT resources are pooled, allowing services to be widely deployed or rapidly shared in response to changing healthcare business and regulatory requirements (Liu & Park, 2013). Also, one of the significant advantages of using cloud computing in healthcare services relates to supporting energy saving and

moving to green computing. It will reduce electricity expenses and resources required to cool computers within data centres (Devadass et al., 2017).

Furthermore, using cloud computing in small hospitals represents an excellent opportunity to overcome current obstacles, such as not having internal IT staff to maintain and service in-house infrastructure for laboratories and medical practices. Thus, reducing infrastructure expenses and IT repairs can mitigate various difficulties in terms of EHR adoption (Schweitzer, 2011; Zhang, 2010). On the other hand, hospitals that are more prominent observe cloud computing as an opportunity to provide ample data storage for IT applications. From the IT manager's perspective, cloud computing can provide the scalability, flexibility and cost efficiency required within the infrastructure (Barua et al., 2011).

Chen et al. (2012) emphasised the extensive benefits of using cloud computing in healthcare services. They highlighted that cloud computing provides the necessary infrastructure for electronic health records because of its flexibility and accessibility.

Cost saving is one of the essential advantages of using the cloud computing model (Cervone, 2010). Operational duties and transactions are moved to the cloud service provider which is then responsible for on-going maintenance of the hardware used by the cloud. Marston et al. (2011) pointed out that cloud computing reduces costs by balancing capital costs with operational costs. As for the healthcare provider, they can benefit from lowering the cost of a wide range of IT software licences which need to be purchased on an annual basis to avoid any service interruption.

Deploying a cloud-based solution in the healthcare domain could address many of the existing limitations, such as those outlined in [Table 2-1](#) .

Benefits	Sources
Support and enable a patient-centric healthcare system.	Barua et al. (2011); Li et al. (2010); Devadass et al. (2017)
Promote enhanced data availability due to the allocation of more resources to avoid data being offline (e.g. redundancy servers), implementation of disaster recovery and continuity practices.	Shini et al. (2012); Ahuja (2012); Mxoli et al. (2014); Masrom & Rahimli (2014). Devadass et al. (2017)
Support rapid provisioning and interconnectivity of electronic resources.	Shini et al. (2012); Liu & Park (2013); Uta (2014); Devadass et al. (2017)
Allow scalable and elasticity demand for e-Health services. Healthcare professionals will be able to attend to their patients from anywhere at any time.	Ahuja (2012); Liu & Park (2013); Mxoli et al. (2014); Devadass et al. (2017)
Enable IT departments (at healthcare institutions) to reduce reliance on in-house expertise in data security. The key elements of security can be left to specialists at the data centre via Service Level Agreements that can be periodically audited.	Liu & Park (2013); Masrom & Rahimli (2014); Devadass et al. (2017)
Improve data quality operations, such as reducing the need for duplicate patient records currently stored in multiple, independently managed databases.	Shini et al. (2012); Uta (2014); Devadass et al. (2017)
Improve the patient quality of service and reduce overall healthcare costs.	Shini et al. (2012); Ahuja (2012); Mxoli et al. (2014); Masrom & Rahimli (2014).
Complement value-based, patient centric care and help reduce administrative burdens as well as benefiting billing and reimbursement processes through the Cloud-based interoperability.	Medical White paper (2018)

Table 2-1 Examples of Key Benefits in a Cloud-based Healthcare System

2.4.2 SWOT Analysis for Using Cloud Computing in Healthcare Sector

Currently, the healthcare sector has to plan to move to the cloud computing environment to enhance communication within healthcare establishments and facilitate accessibility to patient records. Thus, it is necessary to identify the strengths, weaknesses, opportunities and threats concerned with the adoption of cloud computing

services. SWOT analysis is a strategic planning method to evaluate the strengths, weaknesses, opportunities and threats that are involved in a project (Masrom and Rahimli, 2015). It considers the internal and external factors which encourage or discourage project objectives. [Table 2-2](#) shows the results of SWOT analysis performed for cloud computing in the healthcare sector (AbuKhoussa et al., 2012; Bamiah et al., 2012; Masrom and Rahimli, 2015; Devadass et al., 2017).

<p><u>Strengths</u></p> <ul style="list-style-type: none"> • Using cloud computing in healthcare can lead to cost reduction because start-up expenditure is not required (Masrom and Rahimli, 2015). • Flexibility and resilience in disaster recovery by enhancing data availability due to the allocation of more resources to avoid data being offline (Devadass et al., 2017). • Maintenance cost reduction as most of the maintenance is provided by cloud provider (Devadass et al., 2017). • Energy saving as it involves decreasing the additional cost of energy consumption because cloud is based on the network environment so mainly allows for energy consumption to be decreased (Masrom and Rahimli, 2015). • User-friendly because people are aware of smartphone applications (Masrom and Rahimli, 2015). • Ease of access to the patient's records anytime and anywhere leads to increased collaboration among doctors and patients, so the quality of services to patients will be improved (Bamiah et al., 2012; Devadass et al., 2017). 	<p><u>Weaknesses</u></p> <ul style="list-style-type: none"> • Many hospitals do not have Internet connection to connect to the cloud, so it is very hard to implement cloud computing. Internet connection is a fundamental requirement for connecting to the cloud and using cloud services. Therefore, without Internet, the implementation of cloud computing for health sector is impossible (Masrom and Rahimli, 2015). • Employee readiness to accept and use new technology within the work environment is necessary (Lian et al., 2014; Alkhater et al., 2017). • IS staff need to have sufficient knowledge, awareness and skills to adopt cloud computing (Lian et al., 2014). • Technology readiness, existence of the IT infrastructure and human resources can affect the implementation of cloud technology (Alkhater et al., 2017).
<p><u>Opportunities</u></p> <ul style="list-style-type: none"> • Trainees are afforded more opportunities to learn new technology where cloud computing healthcare is provided (Masrom and Rahimli, 2015). • Because cloud computing is provided by a third party, if any problems occur, the cloud provider expert will provide a quick solution without interruption to the hospital service (AbuKhoua et al., 2012). 	<p><u>Threats</u></p> <ul style="list-style-type: none"> • Data security of patient data kept and processed in the cloud is very sensitive and valuable so security in the cloud is very important. It is, therefore the main barrier in adopting cloud computing in the healthcare sector (AbuKhoua et al., 2012) • Fears and worries about the PATRIOT Act in U.S influence the decision of EU cloud customers in using the cloud as a service (Berry and Reisman, 2012). • Transferring health data among various legal and regulatory jurisdictions is very critical and requires deep understanding of cloud outsourcing contracts (Iyer & Henderson, 2012).

Table 2-2 SWOT Analysis for Cloud Computing in the Healthcare Sector

The results of the SWOT analysis revealed that the healthcare sector could make significant progress with the cost reduction model and increase the quality of services. Lower investment in the infrastructure, easy and fast access and optimising resources are all benefits of the cloud computing solution for the healthcare sector. In terms of migrating health care services to the cloud, Software as Services (SaaS) and Infrastructure as Service (IaaS) will be widely used and implemented because they can be customised according to the health center's needs and patient requirements.

2.5 Risks of using Cloud Computing in Healthcare

Adopting cloud computing presents various risks which need to be addressed before the adoption process. Therefore, developing strategies or a framework to enhance security can directly influence cloud computing's adoption rate. Also, if cloud computing for healthcare is to be fully utilized, various issues will need to be considered. According to Liang et al. (2017), some of those issues are related to management, technical, security and legal risks. Each one of these needs to be addressed in detail. Therefore, risk management standards were studied to understand the techniques used in managing risks.

2.5.1 Management Risks

Health care management is one of the top priority areas in many developed countries. There is an increased demand to help those countries, especially those with an increased population who require medical care and resources such as professional doctors and nurses, financial support and community care (Sultan, 2014). Such circumstances encourage many health providers to search for advanced and economic solutions to address this growing problem. Cloud computing is likely to provide a suitable solution for these issues. However, there are risks and challenges associated with the adoption of cloud computing.

The use of cloud computing for personalised medicine requires active management of vast and sensitive datasets. Vast datasets are characteristic of the big data landscape

that exists today. As data sets continue to grow, it is increasingly challenging to maintain privacy for genomic data that is shared across computer networks (Chow-White et al., 2015). In addition, to manage the challenges associated with extensive data sets, other issues exist, such as operating the versatility across different environments, scaling to accommodate large data centres, automating to create self-managed environments, and integration of non-cloud products into the cloud architecture (Joseph and Brown, 2017). Personalized medicine involves collaboration across different entities, so overcoming some of the managerial challenges is vital for continued growth and success (Joseph and Brown, 2017).

Another management challenge can be seen in employee readiness to accept and use new technology within the work environment. It is important that senior management provides positive leadership and support to accept cloud computing as a new service because it will encourage employees to embrace it as a new way of increasing the quality of work (Lian et al., 2014; Alkhater et al., 2017). Therefore, senior management plays a significant role in the acceptance of new technology at the organisational level. Support from senior management is necessary for executing change and facilitating the adoption of the cloud technology in enterprises. In addition, the IS staff need to have sufficient knowledge, awareness and the necessary skills to adopt cloud computing, so that organisations will have more confidence throughout the adoption process (Lian et al., 2014).

According to Alkhater et al. (2017), another challenge relates to technology readiness; the existence of the necessary IT infrastructure and human resources which can affect the implementation of cloud technology. Access to cloud services depends on internet connectivity. Therefore, a good internet connection, high bandwidth and internet speed all play an important role in an organisation's decision to employ cloud services. Prior studies have concluded that organisations that have a robust technical infrastructure and the necessary technical skills are more likely to employ a new technology (Alkhater et al., 2017).

In summary, the key potential risks in terms of management are related to senior management support, human readiness, technology readiness and employee awareness in terms of cloud computing services and internet connection speed.

2.5.2 Technological Risks

The technology issue plays a significant role in terms of adopting any new technology in any organisation. Regarding adopting cloud computing in healthcare services, patient data security and privacy is one area of considerable concern. Rubin (2010) pointed out that it is necessary to address six significant points of risk related to health IT structure before adopting cloud computing within health care services. Those were: regularity risk, performance, intellectual property, liability, business continuity and enforcement (Rubin, 2010). Regularity risk includes encrypting data and preventing unauthorised access.

Chang et al. (2007) discussed how IS complexity and compatibility will affect IT adoption (Lin et al., 2012 ; Liu, 2011). The alignment of IT in large organizations is inherently complex. For cloud computing to deliver real value, it must be aligned to the enterprise rather than simply being a platform for simple tasks, such as application testing or running product demos. Therefore, the issues around migrating application systems to the cloud and satisfying the requirements of key system stakeholders must be explored. These stakeholders include technical, project, operational and financial managers, as well as the engineers who are going to be developing and supporting the systems. Cloud computing is not simply a technological improvement of data centres, but a fundamental change in how IT is provisioned and used (Hosseini et al., 2012). Therefore, the adoption of cloud computing will change the work of various system stakeholders in the enterprise, and this will require considerable effort (Hosseini et al., 2012).

Another challenge can be seen in the system support that will change because administrators will no longer have complete control of a system's infrastructure. Their work could increasingly involve contacting cloud providers and waiting for them to investigate system problems. Such a scenario was reported by Jesper whose

application came under a denial of service attack and it took over 16 hours before the problem was fixed (Hosseini et al., 2012). Jasper application was running on Amazon EC2.

Medical information systems, such as Picture Archiving and Communication systems (PACS), Hospital Information System (HIS) and Radiological Information Systems (RIS), are unique in nature. How to migrate these systems with the cloud computing platform is also a critical factor that organizations need to consider (Lian et al., 2014). This is because system compatibility is another critical factor from the technical perspective. Having cloud computing compatibility with existing systems or applications in the hospital will help make the adoption of cloud computing technology feasible (Lian et al., 2014). Cloud-based solutions have the potential to enable behavioural health providers to adopt state-of-the-art Electronic Health Records (EHR) without incurring fixed costs associated with installation (Carneal et al., 2017). This is because EHR represents a critical tool for collecting, managing and sharing healthcare services information (Carneal et al., 2017).

Costs of the new IT investment play a significant role when hospitals decide to adopt cloud computing technology. This is because establishing a cloud computing platform requires different types of investment in such areas as hardware, software and system integration. The organisation can find costs related to these kinds of projects to be enormous due to the variable nature of the expenses (Lian et al., 2014). Understanding the operational costs of clouds is complicated because the cloud's utility billing model is a shift from capital to operational budgeting, and utility billing has a certain degree of uncertainty that makes it complex to estimate compared to hardware acquisition. The uncertainty relates to: (i) the actual resources consumed by a system, which are determined by its load; (ii) the deployment option used by a system, which can affect its costs as resources such as bandwidth are more expensive between clouds compared to bandwidth within clouds; and (iii) the cloud service provider's pricing scheme, which can change at any time. The consequence is that decision makers are faced with significant uncertainty regarding the best provider and whether cloud adoption is more cost effective than other, more traditional forms of IT provisioning, such as co-location (Hosseini et al., 2012).

In addition, the interoperation represents a huge problem in dealing with patient records. Interoperability is the ability of two or more systems or components (for example, two or more medical informatics systems) to exchange information and use the information that has been exchanged (Lupse et al., 2018). While interoperability is paramount to an efficient system of care and more accurate patient diagnoses, there is some reluctance and fear around embracing technological change (Medical White paper, 2018).

Government agencies, including the Health and Human Services (HHS) and the National Institute of Standards and Technology (NIST), have continued their unrelenting efforts to promote the adoption and popularization of EHRs. These agencies focus on proposing and enforcing new standards to facilitate the interoperability and security of health information, including the Health Level Seven (HL7) international healthcare informatics interoperability standards. Because of the limits of interoperability and security, no single vendor can provide a comprehensive, dominant solution serving both hospitals and smaller outpatient clinics (Jin and Chen, 2015).

Another challenge can be seen in maintaining Health Level-7(HL7) in cloud-based environment. HL7 refers to a set of international standards for transfer of clinical and administrative data between software applications used by various healthcare providers. It was designed to enable interoperability of healthcare information within large hospitals. HL7's focus has been extended to consider the risks of new technologies such as Internet of Things (IoT) and mobile combined with Cloud. A study by Lubamba and Bagula (2017) addressed the issue of interoperability between fog and cloud computing platforms. The results reveal that, for the lightweight devices used by fog infrastructures, "outband" transport over WiFi with edge data translation into HL7 records is a better option than "in-band" transport. Therefore, integrating HL7 into cloud-based environment represents a challenge which needs to be considered in further research (Lubamba and Bagula, 2017).

2.5.3 Legal Risks

The legal issue represents a vital part in the adoption of any new technology due to the rules and regulations involved in using it. Managers and decision-makers need to update their knowledge and understand the various legal aspects associated with it. Also, healthcare is a highly regulated industry as it needs to follow strict traceability, authority and auditability guidelines. Berry and Reisman (2012) emphasised the importance of a legal and regulatory framework as a vital area of consideration for policymakers within the healthcare and IT industry. For example, one key area to consider would be whether to allow personal health data to be transmitted abroad where authorities have different jurisdiction over the data. Therefore, cloud customers need to be fully aware of the rules regarding where their data is held (Berry and Reisman, 2012). Although cloud providers guarantee data protection in data centres stored outside of Europe, there are fears regarding how the PATRIOT Act in the U.S will influence the decision of EU cloud customers to use the cloud as a service (Berry and Reisman, 2012). Thus, one of the crucial challenges for U.S cloud providers is to confirm that cloud customers' data cannot be accessed through the PATRIOT Act and that cloud customers' data will not be accessed as part of intelligence gathering activities. On the other hand, the US has entered the "Safe Harbour" agreement that allows U.S cloud providers to self-certify that they meet the necessary requirements of the EU Directive (Berry and Reisman, 2012).

The U.S and the EU are working on a legislation framework of outsourcing preparations for using cloud computing models and this presents a further challenge as the responsibility between cloud providers and cloud clients becomes unclear (Conbody, 2013). The framework on health management, medical data access and storage capacity will consider how all stakeholders can meet the different conditions and circumstances to permit compliance. The role of cloud contracts that fall within IT outsourcing is significant as well as the roles of cloud clients and cloud providers. Transferring health data among various legal and regulatory jurisdictions is absolutely critical and requires a deep understanding of cloud outsourcing contracts (Iyer and

Henderson, 2012). Those kinds of attitude outspread further than cloud client-provider association to comprise thoughtful facts and ideas of regulation and compliance (Seddon and Currie, 2013).

Even though the U.S and the EU have varying features of cloud policy, both agree regarding the security and privacy of personal data. To create a regulatory framework, they encourage the cloud client and cloud provider to consider individual responsibility and accountability and work as a business partner (Seddon and Currie, 2013).

A survey by Deloitte in 2013 showed that inadequate data security and risk of data availability, open compliance and legal issues, and the risk of losing governance or control over data were the primary challenges facing cloud adoption (Shirazi et al., 2017). Compliance, audit and legal issues around data transfer between different jurisdictions require careful consideration, especially in terms of how data can be audited and logged as per various security compliance requirements. Legal matters represent aspects related to judicial conditions and law, such as multiple data locations and privilege management. Shirazi et al. (2017) highlight that it is necessary to address issues related to forensic and investigation shortcomings in cloud as there is currently no regulation in place to determine how to keep track of the use of the cloud system and what is required to be audited and logged (Shirazi et al., 2017). Given that cloud computing is a relatively new technology, the cyber laws do not yet cover the requirements posed by it (Shirazi et al., 2017).

The lack of legal and judicial requirements and laws also represents a challenge that needs to be considered from a different angle when operating in cloud environments, especially in the healthcare domain. Legal issues have a much more comprehensive impact and expose data to a higher level of risks in cloud environments as opposed to traditional environments (Shirazi et al., 2017).

2.5.4 Security Risks

Using cloud computing in healthcare services can make them vulnerable to potential security threats. Security threats could stem from virtualization, which introduces new vulnerabilities and there could be conflicts between customers and cloud providers who are both attempting to strengthen their security procedures (Hosseini et al., 2012).

To protect patient health information, the United States Department of Health & Human Services established the Health Insurance Portability and Accountability Act (HIPAA) to forbid unauthorised access to information (Osterhaus, 2010). It covers security principles for protecting electronic health information and individual privacy. In particular, HIPAA subsection 506 of 164 includes the use of electronic health information to carry out treatment, payment or health care operation (45 Public Welfare Department of Health and Human Services, 2007).

To support the software engineering effort to establish security requirements from regulations, Breaux et al. (2006) presented a methodology to abstract access rights and responsibilities directly from regulation texts (Breaux, 2006). They applied this method specifically to HIPAA Privacy Rule. Maxwell et al. (2010) presented a manufacture rule framework that software engineers can use in specific compliance requirements for software. They applied the framework to check iTrust, an open source electronic medical records system, for agreement with the HIPAA Security Rule.

Due to the exceptional value of Protected Health Information (PHI), third-party storage servers are a target for hackers and this may lead to a breach in the PHI (Li et al., 2013). Li et al. (2013) emphasise the importance of having fine-grained data access control methods that work with semi-trusted servers to ensure patient data security and privacy. They recommended encrypting the data before outsourcing to the cloud. The PHI owner should decide how to encrypt their files and who will have access to each file only. Those who have the decryption key will be able to access the file. Also, it

allows a patient to revoke access privileges whenever needed at any time (Mandl et al., 2001).

Data security encompasses issues related to confidentiality, integrity, and availability of data. Confidentiality and integrity of data transmission needs to be guaranteed, not only between enterprise storage and cloud storage, but also among different cloud storage services. In other words, confidentiality and integrity of the entire transfer process of data should be ensured (Shirazi et al., 2017). Several studies identify data security as a major concern. For instance, a survey by Forrester in 2013 indicated that 50% of businesses in Europe and North America view security as the number one reason for not adopting a cloud solution (Shirazi et al., 2017). Another survey by Deloitte in 2013 revealed that 78% of IT managers considered that a lack of trust in security was the most significant barrier to the adoption of cloud technologies. In another survey by KPMG in 2014, it was shown that security and data privacy were identified to be of higher concern than cost when adopting a cloud solution (Shirazi et al., 2017). Therefore, it is necessary to have a security mechanism or risk management standard which addresses these potential risks within the cloud environment.

2.5.5 Summary of Risks

A summary of management, technical, legal and security risks is presented in [Table-2-3](#). The table illustrates the risk description, impact, likelihood, countermeasures as well as the relevance and importance of each risk to the Omani context.

No	Risk Type	Risk Description	Impact	Likelihood	Risk mitigation	How important this risk is to the healthcare context in Oman
1	Management	Employee resist change to use new information technology (Lian et al., 2014; Alkhater et al., 2017)..	High	High	Organisational: Government and senior management need to provide positive leadership and support for employees to accept cloud computing as a new service because it will encourage employees to embrace it as a new way of increasing the quality of work	High – this risk has a significant role in the success or failure of a project. Healthcare organisations need to arrange awareness training workshops for employees to accept the change and gain benefits of the new service of information technology
2	Management	IS staff need to have sufficient knowledge, awareness and the required skills to adopt cloud computing (Lian et al., 2014).	Medium	Medium	Human Oriented: Arrange for training courses to provide enough knowledge of skills needed to deal with cloud computing	Medium- Ministry of Health (MoH) in Oman has launched cloud infrastructure to host the ministry's website. MoH needs to provide a training course for IS staff to deal with cloud computing. The medical data is owned by a hospital, used by a doctor and custodian by other hospital. Thus the training courses are needed for data owners, custodians and users.
3	Management	Maintain privacy for genomic data especially with the blending of genomics with Internet technologies which are shared among the network (Chow-White et al., 2015).	Medium	Medium	Technology: Provide Single Sign On to registered users.	Low- It is critical to assure the privacy of patient data among shared network. However, the genomic data is not dealt with in Oman currently.

4	Management	Ensure IS infrastructure deliver the right quality of service.	High	High	Organisational: Organisations need to operate the versatility across different environments; scaling to accommodate large data centres; automating to create self-managed environments; and integrating of non-cloud products into the cloud architecture (Joseph and Brown, 2017).	Low - In Oman there is Oman Data Park (ODP) and Information Technology Authority (ITA) who provide IS infrastructure, and smooth the transfer process. ODT and ITA act like data centre. According to Royal Decree, it is not allowed to hold data in a cloud outside Oman. Thus, risks of storing data abroad are low. In addition, ODT and ITA are compliant with the data centre standard and properly accredited with ISO 20000 for IT service Management, ISO 27001 for information Security Management System.
5	Management	Technology readiness, existence of the IT infrastructure and human resources (Alkhater et al., 2017)	Medium	Medium	Organisational: Organisations need to check their resources in terms of IT infrastructure and humans; whether they can be used to implement e-Gov cloud.	Medium- this is risk relevant to Oman because we have the IT infrastructure However, human readiness is an issue in hospitals as there is a lack of local expertise of cloud infrastructure.
6	Management	High bandwidth and internet speed play an important role in an organisation's decision to employ cloud services.	High	High	Organisational Organisations need to have a robust technical infrastructure and the necessary technical skills to adopt new technical services.	High- this is relevant to Oman as hospitals in the capital already have fibre -optic installed whereas as hospitals in the rural areas suffer from low connection speed. Thus, there is a need to enhance internet connection with suitable bandwidth to be able to accept the new technical service.

7	Technical	IS complexity and compatibility will affect IT adoption (Lin et al., 2012 and Liu, 2011). For instance, migrates medical information system such as (PACS), (HIS) and (RIS) (Lian et al., 2014).	High	High	Organisational: Organisations need to check the alignments of IT application systems to the cloud to check system compatibility in cloud. Having cloud computing compatibility with existing systems or applications in the hospital will help make the adoption of cloud computing technology feasible (Lian et al., 2014),(Lin et al., 2012 and Liu, 2011).	High – because Oman depends on some abroad vendors there is risk of complexity between two vendors. In addition, compatibility issues will raise as two different vendors systems might not be compatible with each other. In addition, Oman has shortage in the in-house experts who are needed to deal with medical information systems such as PACS, HIS and RIS.
8	Technical	Losing control of a system's infrastructure	Medium	Medium	Organisational: Before the adoption process, administrator can identify the system support in the service level agreement (SLA).	Low- it depends on the package that the ministry will choose (a service or infrastructure) as there are different plans suggested to each customer according to their needs. Those services are provided in Oman through Oman data Park (ODP) and Information Technology Authority (ITA).Thus, it depends on the requirement and facilities that MoH needs. Discussed further in Chapter 6

9	Technical	Costs of the new IT investment play a significant role (Lian et al., 2014).	Low	Low	Organisational: Cloud Provider need to calculate the operation costs as adopting cloud computing requires different types of investment in such areas as hardware, software and system integration. The cost can be enormous due to the variable nature of the expenses (Lian et al., 2014).	Not relevant to MoH because its main concern will be on uploading and accessing the medical data whereas Cloud Providers (ODP and ITA) are responsible for calculating the costs.
10	Technical	Interoperation of healthcare systems such as maintaining HL7 in cloud-based environment (Jin and Chen, 2015; Lubamba and Bagula, 2017; Medical White Paper, 2018).	High	High	Technology: Use cloud middleware to ease interoperability issues. Because of the limits of interoperability and security, no single vendor can provide a comprehensive, dominant solution serving both hospitals and smaller outpatient clinics (Jin and Chen, 2015).	High – Healthcare in Oman currently uses the ICD system to record patients’ diagnoses and send ICD messages using the local cloud provider; on the other hand, global hospitals use HL7 to communicate with other healthcare providers. Thus there is a risk of interoperability issues between Oman healthcare and international healthcare providers which can affect the availability of records. Discussed further in Chapter 6
11	Technical	Risks of new technologies such as IoT and mobile combined with cloud (Lubamba and Bagula, 2017).	Low	Low	Technical: Infrastructure to support the impeded system for IoT. Organisational: Those risks need to be added to risk register.	Low- not relevant currently because IoT not implement yet. However, there is a need for Oman to revise the risk management approach once they adopt IoT.

12	Legal	Risk from changes of jurisdiction because the Legal and regulatory framework of where data is held tends to change according to rules and regulation within the custodians' country (Berry & Reisman, 2012).	High	High	Legal: cloud customers need to be fully aware of the rules regarding where their data is held (Berry and Reisman, 2012).	Low- in Oman Cloud provider (ODP and ITA) hold all the data centrally according to Royal Decree.
13	Legal	IT outsourcing is significant as transferring health data among various legal and regulatory jurisdictions is absolutely critical and requires a deep understanding of cloud outsourcing contracts (Iyer & Henderson, 2012). Regulations and compliance need to be considered (Seddona and Currie, 2013).	High	High	Organisational: Provide high level of security with encryption to avoid any leakage during the transferring process.	Low – in Oman is low because it stores data centrally.
14	Legal	Address issues related to forensic and investigation shortcomings in cloud as well as lack of legal, judicial requirements and laws (Shirazi et al., 2017).	Medium	Medium	Legal: Organisations need to consider when operating in cloud environments, especially in the healthcare domain. Rules and regulations need to be expanded to provide more comprehensive impact and expose data to higher level of risk in cloud environment (Shirazi et al., 2017).	Not relevant in Oman currently. In the future, if there is a case which requires exchange of data abroad then there is a gap the legal judicial laws which need to be updated according to the case adopted. Discussed further in Chapter 6

15	Security	Security and privacy of medical data from any threats or attacks are one of the main reasons that prevent many enterprises from employing cloud services (Seddon and Currie, 2013).	Very high	Medium	Organisation: There is a need to decide high level of protection in the SLA to avoid any medical data leakage	Low- storing the data centrally minimize a lot of risks. Also, ODP and ITA-cloud are responsible of managing the data.
16	Security	Third-party storage servers are a target for hackers that may lead to a breach in the PHI (Li et al., 2013).	High	Medium	Technical: Encrypt all medical records before outsourcing to the cloud (Li et al., 2013).	Low- ODP and ITA- Cloud are experienced in data security. The details can be specified as part of SLA
17	Security	Data security encompasses issues related to confidentiality, integrity, and availability of data. These should be ensured not only in an enterprise storage and cloud storage, but also between different cloud storage services (Shirazi et al., 2017).	High	High	Human oriented: Transactional processes need to be carried out by security experts to make sure that there is no illegal activity	High – it will be high in Oman because it is dealing with three objectives of patient data: confidentiality, integrity, and availability.
18	Security	Loss of Encryption Keys: The loss or compromise of cryptographic keys used for encryption, authentication or digital signatures can lead to data loss, denial of services, or financial damages.	High	Low	Technical: There are various ways to restate keys. One alternative is through using PKI. This mechanism assures the activation of the key in a secured channel. Another alternative is via the usage of a mobile SIM card which enables a one-time password to be used in the activation process.	Low as ODP and ITA-Cloud follow high security standards as ISO 20000 and ISO 27000 which provide sense of assurance and security. However, if the risk happens with ODP and ITA-Cloud as they are service provider then the level of risk will change to be high

Table-2-3 Summary of Risks

2.6 Conclusion

This chapter provided a background context related to the use of cloud computing in healthcare. It presented examples of using cloud computing in the healthcare industry. In addition, it emphasised the strategic importance of adopting cloud computing as a service through stating its benefits as well as performing a SWOT analysis for decision makers to consider prior to the adoption process.

Reviewing the literature helped in identifying various types of risks in using cloud computing as a service. However, further work needed to be done to understand how those risks are relevant and important to the Omani context. Therefore, the importance and relevance of each risk were explored in detail.

The next chapter will investigate stakeholders' perception of risk in utilising cloud computing in the delivery of healthcare services in Oman.

3 Chapter 3: Understanding the Perception of Risk Using Cloud Computing in Healthcare in Oman

3.1 Introduction

This chapter will discuss stakeholders' perception of risk in utilising cloud computing in the delivery of healthcare services in Oman. It will present an overview of the healthcare process for primary care in health centres. It will also discuss future projects within the Ministry of Health (MoH, 2017).

An overview of current cloud computing in Oman will be discussed as a potential service to overcome the current limitations of the healthcare systems in Oman. A mixed approach methodology was used; qualitative and quantitative methods were used for collecting data. A preliminary interview with stakeholders was held and two sets of questionnaires were provided for public and healthcare professionals to understand their perception in adopting cloud computing as a service in healthcare. The Undersecretary of Planning Affairs in the Ministry of Health was interviewed to evaluate the findings of the questionnaires. The outcome emphasises the need to find an effective risk assessment methodology to overcome various risks identified. Finally, the findings will be reflected upon and recommendations for the Omani government in terms of areas for improvement will be provided.

3.2 Healthcare in Oman

The Ministry of Health (MoH) in Oman provides healthcare services to citizens and residents through various health care centres and hospitals. Existing information systems within hospitals and health centres are fragmented. For example, the existence of health records in different databases across healthcare establishments as well as the terminologies and codes used to define medical services such as diagnosis and radiology and laboratory investigations complicate efforts to achieve efficient and effective healthcare delivery.

The Ministry has spearheaded four initiatives to resolve the fragmentation of healthcare information systems. The first initiative is the Development of Smartphone Applications (DGIT), which involves the launching of several health-related mobile applications (apps), including “e-health portal” and “e-services” which allow for the searching of drug prices and pharmacies based on location, as well as managing hospital appointments and viewing medical records (MoH, 2017). The second initiative is Consolidating and Standardizing the Database of Diagnosis, Radiology and Laboratory Tests (CSDDRLT) to unify the different databases and standardise the identification codes to facilitate seamless communication between healthcare providers with the aim of reducing misinterpretations (MoH, 2017). The third initiative is Selection and Purchase of International Standards for Connecting Databases and Diagnostic Radiology and Laboratory Tests (SPISCDDRLT). Once terminologies and codes used in the diagnosis, radiology and laboratory databases have been standardized and consolidated in the CSDDRLT initiative, the terminologies and codes will be mapped to known coding standards system (e.g International Classification of Diseases, Tenth Revision, Clinical Modification (ICD-10-CM) to ensure that the healthcare information system is compliant with international norms and facilitating communication with healthcare providers outside Oman (MoH, 2017). The fourth initiative is Disaster Recovery (DR), which is designed to improve data availability when a particular data centre is not operational due to cyber attacks, natural disasters or other reasons (MoH, 2017).

The Ministry has introduced Infrastructure as a Service (IaaS) cloud services hosted by the Government’s Information Technology Authority (ITA) (MoH, 2017). Building on the ITA’s IaaS cloud, Oman’s MoH implements the "Al-Shifa" project, where a patient can book and cancel a medical appointment online 24/7. Patients can also request their medical report and pay online before collecting the medical report in person. However, it appears that Oman’s MoH has not fully utilised the cloud platform in the delivery of healthcare services (MoH, 2017).

The current healthcare system in Oman is mainly non-cloud based and has shortcomings in many areas: (i) Oman's current healthcare system does not adopt Health Level Seven (HL7) which represents an interoperation barrier to communicate with other countries. (ii) it does not support a patient-centric approach, (iii) it does not allow a patient to access his/her medical records online and, (iv) it does not facilitate the process of a patient seeking treatment from other healthcare providers (i.e. it does not enable information-sharing between healthcare providers). Therefore, patients do not have online access to health records outside the country even in situations that require urgent medical treatment (e.g. accidents during an overseas trip). Also, there is a significant number of expatriates (46%) in Oman. These expatriates may need to access their medical health records when they travel home. Currently, healthcare workers, such as medical practitioners, do not have access to a patient's medical history stored within a different healthcare establishment, which can potentially result in fatal outcomes (e.g. a medical doctor is not aware whether the unconscious patient admitted to the emergency department is allergic to a particular medication or not).

According to the National Centre for Statistics & Information in Oman (NCSI, 2017), the country's population is 4, 558, 196 comprising 2, 490, 462 Omani citizens (54%) and 2, 114, 508 expatriates (46%), as of 13th April 2017. The Internet penetration rate in Oman is approximately 80% (3,646,557 users), but only 17, 000 users reportedly access health services online.

Using cloud computing in healthcare (e.g. Cloud-based Electronic Health Records: CEHR) can bring many benefits to healthcare providers and patients, and address existing limitations in the conventional healthcare system.

While the above discussed limitations can be addressed using a cloud-based solution such as CEHR, healthcare providers in Oman are hesitant to migrate to the cloud. Therefore, this research investigates how Omani stakeholders perceive cloud

computing and seeks to understand factors that affect cloud computing adoption for healthcare provision in Oman.

3.3 Research Methodology

Cloud computing is an emerging technology in Oman. Therefore, it is necessary to conduct an empirical study to collect further information to define the problem clearly. The research methodology used in this research is performed in six stages as shown in Figure 3-1. These are research problem identification, research aims, research questions, interviews, questionnaires and research evaluation.

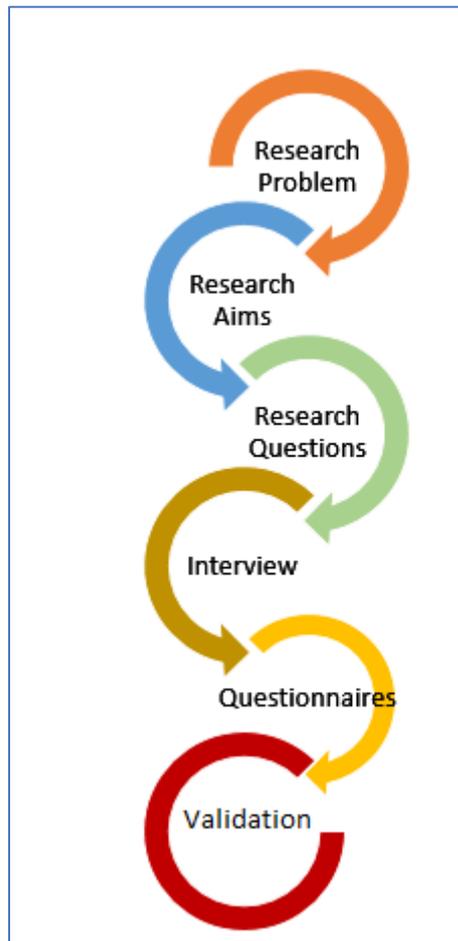


Figure 3-1 Research Methodology Stages

- 3.3.1. Research Problem:** a literature review was conducted to understand cloud computing's background and identify the key benefits of adopting cloud computing in healthcare delivery.
- 3.3.2. Research Aim:** the research aim was to “*Understand the perception of risk in adopting cloud computing in the delivery of healthcare services*”.
- 3.3.3. Research Question:** the main research question is “What are the factors preventing Oman from adopting cloud computing in the delivery of healthcare services?”
- 3.3.4. Data Collection:** a mixed approach was adopted using qualitative and quantitative methods for collecting data.
- Qualitative:* semi-structured interviews were conducted with seven interviewees who were chosen based on their experience in healthcare provision in Oman. They were chosen as an orientation sample who have a general idea of using cloud computing in the delivery of healthcare services.
- Quantitative:* two questionnaires were designed; the first was designed for the public end-users to determine their perception of security in terms of using cloud computing to deliver healthcare services. The second questionnaire was for healthcare professionals and managerial end-users to determine their perception of security when using cloud computing in the delivery of healthcare services, and their perceptions of organisational and environmental factors that may affect cloud computing adoption. This will be addressed further in section 3.6 .
- 3.3.5. Research Validation:** to validate the findings of the preliminary interviews and questionnaires and understand the primary security concerns from the decision-makers' point of view, an interview with

H. Dr. Ali Talib Al Hinai, Undersecretary for Planning Affairs in Ministry of Health in Oman, was conducted.

3.4 Data Collection: Qualitative Semi-structured Interviews

The literature was carefully reviewed regarding the challenges that might prevent organisations from adopting cloud computing as a means of bringing about technological improvement in data centres and how IT is provisioned and used. [Table 3-1](#) provides justification for all parts of the interview questions. The full set of interview questions is available in [Appendix A.1](#). In addition, [Appendix A.2](#) provides a glossary of technical terms, which was provided for the interviewees.

Items	Justification
Part 1: Meeting aim	A short summary about the meeting aims and the research objectives is provided.
Part 2: Role in the organisation	To understand the candidate's role and responsibility within an organisation.
Part 3: Management perspective	To understand management's attitude regarding adopting cloud computing as a service in healthcare in Oman and to understand management support and staff readiness to use cloud computing within their workplace.
Part 4: Security (data storage, process, transfer, access control, procedure)	To understand organisation's security awareness of the security concerns in using cloud computing.
Part 5: Privacy	To understand non-disclosure and cloud provider access to stored data.
Part 6: Technical understanding	To understand organisation's technical knowledge when cloud providers face technical issues preventing them from providing the service.

Part 7: Legal understanding	To understand organisation’s awareness of legal requirements.
Part 8: Risks not specific to cloud	To understand organisation’s readiness to face risks not specific to cloud computing.
Part 9: Further recommendations	As cloud computing is an emerging technology in Oman, it is necessary to establish connections from experts in the field.

Table 3-1 Justification of the Interview Questions

Each interview lasted an average of 35 minutes. [Table 3-2](#) presents the demographic details of each interviewee. The interviews were audio-recorded and transcribed verbatim. Appendix [A.3](#) to [A.9](#) represent the interview transcript for the orientation sample. The transcripts were then analysed to identify the factors that influence the adoption of cloud computing in the delivery of healthcare services. In the semi-structured interviews, a hypothetical case study was used to frame the discussion and obtain insights into the seven interviewees’ perceptions.

Participant	Age Group	Role	Job Tenure	Interview Format	Questions asked
CC01	35-49	Head of Genetics Department in Sultan Qaboos University	More than 5 years	Face-to-face	Parts 1,2,3,5 and 9
CC02	35-49	Associate Professor in Behavioral Medicine Department in Sultan Qaboos University	More than 5 years	Face-to-face	Parts 1,2,3,5 and 9
CC03	20-34	Manager of G-Cloud project in Information Technology Authority	More than 5 years	Face-to-face	All parts
CC04	20-34	Director of eHealth in Ministry of Health in Department of Information Technology	More than 5 years	Face-to-face	All parts
CC05	20-34	Assistant Professor, Science College at Sultan Qaboos University	1-5 years	Feedback via e-mail	All parts
CC06	35-49	Assistant Professor and healthcare consultant and manager	More than 5 years	Feedback via e-mail	All parts
CC07	35-49	Consultant at Gartner	More than 5 years	Feedback via e-mail	All parts

Table 3-2 Demographics of Interviewees

3.5 Hypothetical Case Study

The case study assumes that an Omani resident (either citizen or expatriate), say Patient A, suffers from a malignant head tumour and requires an urgent medical procedure to be carried out. For the medical procedure, say surgery, patient A decides

to travel to a foreign country, say Germany, to carry out the surgery because there is a lack of resources in Oman as only one hospital can perform those kinds of surgeries. Therefore, patients tend to travel to a foreign country if they are unable to schedule urgent surgery in a suitably short timescale. Patient A is unable to access the medical records stored in Oman's healthcare establishments; thus, the hospital in Germany has to conduct various medical tests and procedures (e.g. x-ray examinations). Unless the patient remains in Germany after the surgery, collaboration and communications between the healthcare workers in both Germany and Oman will be required to provide seamless follow-up post-surgery care. This is currently not possible in the existing Omani healthcare system.

3.5.1 Findings

Interviewees were generally positive about utilising cloud computing in the delivery of healthcare services but a number of concerns were raised as presented in the remainder of this section.

3.5.1.1 Human Factors

Human factors include the attitude, perception and the willingness of (human) users in terms of accepting and adopting new technologies, and, as noted by the interviewees, there could be a range of reactions to any consumer technologies. For example, interviewee CC07 explained that resistance to change could be an inhibiting factor as, *"Asking someone to give up part of their job is always difficult and human nature shows that a defensive position is often taken as people do not like change"*. While enhancing the job with better technology represents an advantage for the organisation, losing control is another barrier which needs to be addressed. The system administrator will lose part of the control over their system when they move to cloud-based one as they will not control where data is stored or processed. Although they can specify their preferences in the service level agreement, in satisfactory level, they will not have the same degree of control as they would in an ordinary legacy system.

The research findings also suggested the need to educate relevant stakeholders, such as those in the healthcare systems and governments, about the benefits of deploying cloud computing in the delivery of healthcare services (CC01, CC02, CC05, CC06, CC07). For example, interviewees CC05 and CC07 noted that, “*Migrating partially to cloud computing will give medical team a chance to inspect the reality of what cloud can and cannot do*” (CC05) and “*Many departments welcome use of cloud based applications as they frequently offer more modern capabilities, frequent upgrades keeping the functionality current and they are not waiting on IT to deliver this*” (CC07).

In asking about the department reaction for migrating to a cloud service provider and how the level of access to their data will be different in the cloud compared with the current system, it was clear that there will be many challenges which need to be addressed.

The IT professional skills need to be updated and refreshed to deal with the new services. The cloud computing services offer several advantages to IT professionals that can enhance their overall capabilities due to easy access to several expensive information technology enabled resources which would otherwise not be affordable in a traditional computing environment. Therefore, this can result in improved flexibility and efficiency leading to higher overall performance in the job. The superior benefits and inherent characteristics associated with perceived usefulness made cloud computing services more acceptable. Hence, service providers need to focus on designing cloud computing solutions that meet IT professionals' requirements for improving their productivity and performance (Sharma et al., 2016)

In addition, IT professionals need to be aware of potential risks and challenges, so they will know how to act to reduce the anticipated challenges. One of the interviewees suggested that the government should consider, “*Providing certification and workshop to understand workflow of cloud system to eliminate potential challenges such as*

incompatibility issues, security and privacy issues, reliability issues, availability issues and network connectivity issues etc.” (CC06).

It is also essential that all stakeholders (e.g. healthcare professionals and patients) have confidence and trust in the security of their data in the healthcare cloud network (CC04).

3.5.1.2 Technological Factors

Technological factors include risks relating to the underlying technologies, such as vulnerabilities in the cloud infrastructure that can be exploited by an attacker. Echoing findings from Lian et al. (2014), data confidentiality, integrity, availability and security are key concerns raised by the interviewees.

According to CC01, CC02, the general consensus is that medical doctors support the migration of healthcare services to the cloud. However, they also reinforced the need to ensure confidentiality of patient medical information (e.g. medical history). This is not surprising as leakage of information, such as HIV-positive and mental illness, may jeopardise the patient’s employment and social status. For example, it was explained that, “...*Because confidentiality is a crucial issue. Patient care is different from other cases. Some people do not like others to know their condition or their diagnosis of certain disease because of social stigma or something like that as it can affect their work and social states in the community. So this should be considered crucial actually.*” (CC02)

One of the key benefits of migrating healthcare services to cloud computing is to maximise the provision of healthcare services to patients and reduce inefficiencies. Another potential benefit is increased research collaboration and information sharing with other healthcare researchers, such as the scenarios raised in the hypothetical case

study. Similar sentiments were shared by CC01 and CC02. For example, it was noted that:

“...the security for the patient’s secrets and states should be kept confidential. But it is a good idea to communicate with other colleagues in other hospitals and other countries. To exchange idea and opinion about certain conditions and cases.”

(CC02)

From CC02’s comments, a paradox of confidentiality and availability arise. On the one hand, there is a need to have patient records available for other colleagues to exchange ideas. On the other hand, anonymisation and information partitioning are important to maintain the privacy and confidentiality of a patient’s file. According to Sahi et al. (2018), data confidentiality and privacy are somewhat similar, since hypothetically, no one is supposed to see the data. Once data securely arrives at the core network, its protection, privacy preservation, processing, and proper distribution takes place. Access control, user anonymity, and other privacy preservation requirements need to be met. At this point, a distinction is made between those who are allowed access to health records and those who are not. In addition, a distinction arises between who is allowed to see patient-centric information (name, ID number, etc.) and who is allowed to see healthcare centric information (Protected Health Information) (Sahi et al., 2018).

Interviewees (CC01, CC02) also remarked that it is important for prospective healthcare cloud providers to ensure data-at-rest encryption, data portability, data integrity and backup. Data backup is particularly important, for example, during times of natural disaster, as it helps to ensure that medical doctors and other allied health workers have access to patient and other crucial information when their own system is down. One of the interviewees, however, raised concerns that a data recovery plan may not be provided by-default:

“They have to come with the first request: what they want. If you are ministry X, then you would know you need a backup. You would know any cluster environment. And you are probably looking for Data Recovery service. So you put that as requirement as it does not come as default so you’ve got them all.”(CC03)

One interviewee (CC03) explained that Oman’s Information Technology Authority (ITA) adopts the International Information Security Standard (ISO 27001), and explained that there are concerns about the data being hosted in overseas cloud servers:

“..at this point we do not have data outside. It is all in Oman because of security promising it should be in Oman. As I said at the beginning we have to follow the government security rule that information security rules released in 2013. But it been released by our security advisor division in ITA.” (CC03)

According to Oman policies, Oman prohibits hosting any kind of data for the government sector in public Clouds (Microsoft, Google, or any free or commercial cloud service existing outside Oman). However, there are various partners providing such services in Oman, for example (Oman Data Park (ODP) and Information Technology Authority- G-Cloud (ITA G-Cloud), or other private partners existing in Oman. The data are stored in the cloud based on the service type and requirements of the customers whether they are requesting IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service) or SaaS (Software-as-a-Service). However, to maintain confidentiality, integrity and availability in cloud services, there should be NDA (Non-Disclosure Agreement) form signed between two parties (service owner & service requester) to reserve rights at both ends.

In terms of the backups, whether stored in Oman or abroad, a representative from ITA (Information Security Department) team responded thus: *“Backups are all maintained in Oman too as long as confidentiality of data should be kept in a secure zone and unreachable by unauthorized entities. They believe maintaining backups for any*

country shouldn't be externally because this shall threat the data integrity, confidentiality and availability. Maintaining the data policy during natural disaster might be exist in Ministry of National Economy (MoNE) because they are handling backup side so whatever is implemented there, it will be under their responsibility".

Another interviewee (CC06) also emphasised the importance of having in place sound data security measures, which are in compliance with the relevant standards.

3.5.1.3 Organisational Factors

Organisational factors include a range of organisational conditions, such as management support, organisational resources, and organisation culture. A number of interviewees noted that their organisations recognised that implementing healthcare cloud services in the country can provide benefits, such as scalability, cost-efficiency and enhanced healthcare services and enhanced quality of experiences (CC01, CC03, CC05, CC06):

"Ah.. it's fantastic idea and something that we will be moving to it in any way. We can't avoid it; technology is improving at high speed and we are already moving to it in other fields and areas. And healthcare is also already moving to it." (CC01)

"I do agree about that this will be defiantly a big jump in terms of quality in healthcare in Oman in terms of benefits and adequate resources." (CC03)

"Migrating healthcare services to clouds becomes more and more attractive IT option to cut costs, support on-demand provisioning, diversify infrastructures, and obtain higher levels of flexibility and security." (CC05)

3.5.1.4 Environmental Factors

A number of interviewees cited the timeliness of introducing cloud services to the delivery of healthcare services, due to the interest of the government. For example, one interviewee (CC04) mentioned the Al Shifa project. This project seeks to implement an electronic service that allows a user to access his/her medical record through the ministry portal (www.moh.gov.om), which is hosted within G-Cloud:

“We are not providing eHealth services in terms of health services. We are providing e-services in terms of just communicating with health establishment. To request an appointment or can cancel an appointment or reschedule an appointment. We do not store the medical records of a patient online.” (CC04).

The interviewee also cited other ongoing government initiatives in this area by using Al Shifa project. Al Shifa project can gather all fragmented patient health records in one place. It does not store patient medical records online, but it facilitates ease of access to patient records within different health establishments:

“The ID card does not store the medical history. It is read from Archive of health information system through the portal. And it read chart by chart it doesn't read a combination of both records so far. Because still did not unified the patient record. We will be doing in stages later.” (CC04)

The ID card represents the civil identification number which all citizens and residents are required to have whenever they visit the health centre for medical treatment. Therefore, it is a unique identification per person and no one will have the same number.

A summary of the interviews' findings is presented in [Table 3-3](#) according to the factors, opportunities, challenges and sources from the interviews.

Factors	Opportunities	Challenges	Source from Interview
Human	Save a lot of time to take care of the patient's health.	Medical teams tend to resist change and new information technology.	CC05,CC06 CC07
	Increase research collaboration with other researchers in a similar field of the patient's case or treatment plan.	Both healthcare professionals and patients must trust the cloud network security to protect personal data for it to work.	CC05 , CC06 ,CC07
	Give medical teams a chance to inspect the reality of what cloud can and cannot do.	Medical doctors support migrating healthcare services to cloud computing subject to the confidentiality and integrity of patients' data.	CC02, CC05 CC06,CC07
Technology	Speed up the treatment plan for patients due to the secure connection and data availability.	Medical teams place emphasis on the availability of medical information during any natural disaster that might occur.	CC01,CC02
		Having access to the right medical information and information belonging to the right patient.	CC01,CC02
	Data in the cloud will be stored locally in Oman.	Data security and confidentiality are of a primary concern.	CC01,CC02, CC03
		Users must use strong passwords and authentication measures.	CC01,CC02, CC03
		Cloud providers should provide backup, encrypt data, make it portable and provide data integrity.	CC01, CC02 CC03
		The cloud provider must ensure data security measures to prevent unauthorized access, and protect accurate and reliable patient data. It should assure availability, confidentiality, and integrity of	CC01,CC02, CC03

		electronic protected health information through a series of administrative, physical and technical safeguards.	
Organisational	Cloud computing quickly brings in whole economies of scale with most cloud services providers charging on a pay as you go basis, thereby eliminating wastage of unused resources.	Will top management support cloud computing migration?	CC01,CC03, CC05, CC06
	Achieve scalability, cost-efficiency, and higher performing healthcare services.	Are there adequate resources to migrate healthcare services to cloud computing?	CC01,CC03, CC05 ,CC06
	Educating and training medical teams about cloud benefits.	Will the perceived benefits of utilizing cloud computing reduce operating costs in healthcare?	CC05 ,CC06
	Provide certification and workshops to understand the workflow of the cloud system to eliminate potential challenges such as incompatibility issues, security and privacy issues, reliability issues, availability issues and network connectivity issues.		CC05 ,CC06
Environment	Having unified medical records as one of the government policies.	Medical/clinical data are not hosted in the government cloud.	CC04

Table 3-3 Summary of Interviews Findings

The interviews' findings reveal that there is a positive attitude regarding the benefits of using cloud computing but there are various risk factors; human, technology, organisation and environment, that need to be investigated further. The next task is to conduct a detailed questionnaire for public and healthcare professionals/managers to identify stakeholders' perceptions regarding these risk factors.

3.6 Data Collection: Quantitative - Creating Questionnaires

To determine perception and/or concerns of the public and healthcare professionals in utilizing cloud computing for healthcare services, two sets of questionnaires were created for the public in Appendix [B.2](#) and health care professionals in Appendix [B.3](#). Both questionnaires are written in English and Arabic. The steps- from one to seven- explain the processes carried out in creating both questionnaires. [Table 3-4](#) presents the justification for each part.

Step 1: A brief introduction about the researcher (i.e. researcher's name, university name) and the length of the questionnaire with the expected time is given. In addition, a short definition of cloud computing is included.

Step 2: Explains the objectives of the research.

Step 3: Confidentiality and privacy guarantee was essential to obtain participant trust and clarify that their opinion will be utilized for academic research only.

Step 4: The survey started with demographic questions to increase response rates and lower drop-out rates, as recommended by Teclaw et al. (2012).

Step 5: After the demographic questions, the structure of the questionnaire proceeded with questions about the perception of adopting cloud computing services in the delivery of healthcare, as shown in [Table 3-4](#).

Step 6: Questions were underpinned with a review of the existing literature (ENISA, 2012; Mxoli et al., 2014) to validate research aims and objectives for every concept.

Step 7: Finally, both questionnaires were translated from English to Arabic in order to improve the quality of response. Thus, the participants could view each statement in English and Arabic.

Items	Justification
Part 1: Demographic questions	To increase response rates and lower drop-out rates as recommended by Teclaw et al. (2012).
Part 2: Yes/No questions about IT experience and cloud computing awareness	To classify those who have IT experience and knowledge about cloud computing services.
Part 3: Internet Based Services	To recognise to what extent participants use internet-based services within their work or daily activities.
Part 4: Human	To detect human readiness and willingness to use cloud computing in healthcare. Also, to view their perception of privacy.
Part 5: Privacy	To seek information about privacy perceptions regarding their personal details, credit card details and health records details.
Part 6: Technology	To understand participants' perceptions and concerns about the use of cloud computing in the delivery of healthcare services (confidentiality, integrity, availability, data security, complex, compatibility and cost).
Part 7: Organisational (for healthcare professionals only)	To identify healthcare professionals' perceptions in migrating healthcare services to cloud computing (regarding various issues such as relative advantage, top management support, adequate resource and benefits).
Part 8: Environmental (for healthcare professionals only)	To identify healthcare professionals' perceptions in terms of government policy and perceived technical competence.

Table 3-4 Questionnaire Structure

The questionnaires designed to collect data for this research were divided into eight parts. The questions in each section had an alpha character and a numeric number, the former indicating which section (T=Technology; H=Human, P=Privacy, I=Internet Based Services, O=Organisational and E=Environmental) and the latter being a simple sequence.

The questions were adopted from Lian et al. (2014), who investigated the critical factors that affected the decision to adopt cloud computing technology in developing countries, specifically in Taiwan's hospital. The questions used in Human, Technology, Organisational and Environmental parts are adopted in this research.

In addition, Wijaya et al. (2014) discussed Indonesian awareness of health records stored in cloud computing through a survey. The survey conducted consisted of three components (hospital's IT staff, patients who have an IT background, and patients who do not have an IT background). The Yes/No questions, Internet-based services and Privacy questions of Wijaya et al. (2014) were adopted in this research.

Singh et al. (2014) used a survey to identify factors related to the organizational information security because technical solutions alone are not sufficient to address the information security challenge. It has been argued that organizations also need to consider the management aspects of information security. Hence, this research adopted 'top management support' for the organisational questions' parts (the same questions are used by Lian et al. (2014)).

Chang et al. (2007) investigated factors affecting the adoption of electronic signature in hospitals. They used a framework of Technology–Organization–Environment (TOE) in IS discipline for adopting an innovative technology and indicated the critical factors that affect the adoption decision. TOE is consistent with the theory of innovation adoption in technological characteristics and internal and external characteristics of the organization (Chang et al., (2007). In this research, the questions on the adequate resource and government policy were adopted from Lian et al. (2014).

Appendix [B.1](#) provides a full justification of the main purpose of each question and adopted sources for each section. There were two questionnaires; Public questionnaire (Appendix [B.2](#)) which consisted of parts 1 to 6 and Healthcare professional questionnaire (Appendix [B.3](#)) which consisted of two extra parts: 7 and 8.

Both questionnaires were created using Google Forms, which resulted in a URL link for each questionnaire. The URLs were then distributed through social network services (WhatsApp) on the 8th January 2016. WhatsApp was chosen because it is one of the most widely used instant messenger applications with more than one billion users (Rösler et al., 2018). It represents an important part of daily life to easily communicate with multiple participants at the same time via group chats on smartphones. It allows sharing of text messages and attachments, such as images or videos for both direct communication and group communication (Rösler et al., 2018). Although WhatsApp provides end-to-end encryptions, it has many security and privacy issues which need to be addressed. For instance, by using WhatsSpy tool, it is possible to track the online activity of every WhatsApp user around the world by continuous monitoring of the current online status. In addition, the user has no capability to change that setting, thus currently possessing no countermeasure against this form of tracking (Rottermanner et al., 2015). This research used WhatsApp as a distribution method to reach the maximum number of participants only. The participant followed a link which led to the questionnaire. They did not complete it in the WhatsApp itself.

A brief description was provided for the participants stating which URL to use. For instance, the general public are eligible to participate in the Public questionnaire, Appendix [B.2](#) and those who work in the healthcare are eligible to participate in the Healthcare professional questionnaire (Appendix [B.3](#)).

In addition, the Office of the Advisor for Academic Affairs was contacted in order to obtain permission to distribute both questionnaires via official emails within Sultan

Qaboos University for students and staff as well as for Sultan Qaboos Hospital (Appendix [B.4](#)).

Data collection concluded in June 2016. According to Hair et al. (2010), a sample size should be 100 or more to obtain a loading factor of 0.5 in order to be considered as being of practical significance. Therefore, a kind reminder was sent out every two weeks to encourage participants to fill out the questionnaires. A total of 400 members of the public and 150 healthcare professionals participated in the survey. Appendix [B.5](#) represents the demographic data of both sets of respondents.

3.7 Data Analysis and Results

3.7.1 Reliability and Validity

The data was saved in Microsoft Excel, and coded before importing to IBM SPSS version 23 for statistical analysis. Exploratory Factor Analysis (EFA) was used to validate the developed dimensions in order to determine whether the sample was adequate. In addition, EFA can be used to examine the interrelationships between items, reduce their number, and form them into constructs (Hair et al., 2010). Hair et al. (2010) explained that even though a factor loading as low as 0.3 and 0.4 is acceptable, a loading factor value greater than 0.5 is essential for practical significance.

Using EFA to analyse the responses to questions in Parts 3, 4, 5 and 6 resulted in ten constructs (Appendix [D.1](#)) with new groupings for Confidentiality, Integrity and Availability with a factor loading of 0.928. The Internet-Based Services were segregated into three groups, namely: Internet Based Services with a factor loading of 0.681, Social Network with a factor loading of 0.500, and Business Network with a factor loading of 0.500. Similarly, Complexity and Cost were grouped together as one construct with a factor loading of 0.882. Data Security and Compatible remain in the

same construct, as suggested in the literature (Lian et al., 2014). A new construct was created, namely: Cloud Provider with a factor loading of 0.607. Table 3-5 presents the factor loading and sampling adequacy for each construct. As the measure of sampling adequacy of all constructs exceeded the minimum acceptable value of 0.5, it implies that variables under each construct are sufficiently inter-correlated.

The reliability of EFA was measured by calculating Cronbach's alpha, which is a reliability coefficient measure that ranges from 0 to 1. Cronbach's alpha is calculated using the formula:

$$\alpha = \frac{N \cdot \bar{r}}{(1 + (N - 1) * \bar{r})}$$

where N = number of items

\bar{r} = average correlation

For a variable to be considered reliable, its Cronbach's alpha must be above 0.7 although a value between 0.6 and 0.7 is acceptable in a preliminary study (Hair et al., 2010; Tabachnick and Fidell, 2001). As observed from Table 3-5, most of the constructs were considered reliable since their Cronbach's alpha values range from 0.607 to 0.946. Social Network and Compatible constructs were removed since their values were below 0.6. Appendix B.6 presents the rotated component matrix for public and healthcare professionals.

No	Construct	Item	Factor loading	Sampling Adequacy	Cronbach's Alpha (α)
1	Data Security	T14	0.595	0.955	0.946
2		T15	0.739		
3		T16	0.730		
4		T17	0.809		
5		T18	0.841		
6		T19	0.867		
7		T20	0.862		
8		T21	0.777		
9		T22	0.796		
10		T23	0.806		
11		T24	0.644		
12	Confidentiality, Integrity, Availability	T3	0.592	0.928	0.919
13		T4	0.670		
14		T5	0.766		
15		T6	0.750		
16		T7	0.753		
17		T8	0.838		
18		T9	0.788		
19		T10	0.797		
20		T11	0.741		
21		T12	0.630		
22	Complex & Cost	T25	0.635	0.882	0.897
23		T26	0.636		
24		T27	0.611		
25		T28	0.638		
26		T29	0.556		
27		T33	0.652		
28		T34	0.657		
29		T35	0.654		
30	Internet Based	I4	0.626	0.681	0.686
31	Services	I5	0.598		

32		I7	0.713		
33		P4	0.658		
34	Privacy	P1	0.791	0.689	0.681
35		P2	0.813		
36		P3	0.564		
37		P5	0.652		
38	Business Network	I6	0.734	0.500	0.718
39		I8	0.735		
40		I2	0.609		
41	Human	H2	0.725	0.500	0.725
42		H3	0.650		
43	Cloud Provider	T1	0.610	0.500	0.607
44		T2	0.628		

Note: * Cronbach's alpha level $\alpha \geq 0.9$ is considered to be an excellent indicator of internal consistency
 ** Cronbach's alpha level $0.7 \leq \alpha < 0.9$ is considered to be a good indicator of internal consistency
 *** Cronbach's alpha level $0.6 \leq \alpha < 0.7$ is considered to be an acceptable indicator of internal consistency (Choo *et al.*, 2015)

Table 3-5 Factor loading and Cronbach's Alpha for Public and Healthcare Professionals

The findings from the analysis of the healthcare professionals' data for parts 7 and 8 are presented in [Table 3-6](#). Constructs with a factor loading of less than 0.6 were removed. Initial groups mostly remained the same with the exception of the environmental factors as two items were excluded. Appendix [B.7](#) represents the rotated components for healthcare professionals.

No	Construct	Item	Factor loading	Sampling Adequacy	Cronbach's Alpha (α)
48	Benefits	O12	0.783	0.923	0.953
49		O13	0.739		
50		O14	0.825		
51		O15	0.813		
52		O16	0.742		
53		O17	0.788		
54		O18	0.832		
55		O19	0.789		
56		O20	0.701		
57	Gov. Policy	E1	0.628	0.821	0.876
58		E4	0.710		
59		E5	0.746		
60		E6	0.773		
61	Adequate Resource	O8	0.563	0.753	0.837
62		O9	0.636		
63		O10	0.561		
64		O11	0.507		
65	Top Management Support	O4	0.708	0.826	0.898
66		O5	0.766		
67		O6	0.785		
68		O7	0.765		
69	Relative Advantage	O1	0.810	0.756	0.913
70		O2	0.811		
71		O3	0.818		

Table 3-6 Factor loading and Cronbach's Alpha for Healthcare Professionals

Four academics were consulted to independently verify that the techniques were applied appropriately and that the results were valid and reliable. The assistance of Dr. Asma Al Zidi and Dr. Sujeet Kumar Sharma from Sultan Qaboos University, Dr. K. Srinivasan from Higher College of Technology and Dr. Andreas Artemiou from Mathematics School at Cardiff University are acknowledged.

3.7.2 Radar Chart

Radar chart is one of the most widely used methods for evaluation (Shaojie et al., 2017). The most distinct characteristic of radar chart is its intuitive visualization through which the status of the evaluated object can be displayed intuitively (Shaojie et al., 2017). The author selected the radar chart to visualise the perceptions of the public and healthcare professionals regarding each statement via numerical proportions.

3.7.2.1 Construct for Radar Chart

Once the validity and reliability of the results were established, basic Excel analysis was conducted to identify the perceptions for all statements in each construct. Responses such as 'not applicable' and not answered responses for both surveys were excluded because the numbers were small (around 10% within public and 5% among professionals). Then, the percentage of agree (strongly agree + agree) against the percentage of disagree (strongly disagree + disagree) was compared. The remaining percentage relates to those responses that neither agreed nor disagreed, but these are not shown in the table (Appendix [B.8](#) for Public and healthcare professional common parts and Appendix [B.9](#) for Healthcare professionals). Radar figures were used to present the results for each construct. For example, in Data Security construct, the radar chart ([Figure 3-2](#)) includes all questions loaded based on SPSS analysis. [Table 3-7](#) represents the percentage response for Data Security.

Data Security	Public % Agree	Professional % Agree	Public % Disagree	Professional % Disagree
T14: Cloud computing technology provides a secure channel for transferring medical data across different sites.	56	69	14	12
T15: When using cloud-computing technology, there is a risk of your medical data being stolen.	50	45	23	30
T16: You do not think it is safe to use cloud-computing technology in healthcare because of security concerns.	43	44	29	26
T17: You believe by using cloud computing in healthcare there is a significant risk of data loss.	45	44	32	27
T18: You believe by using cloud computing in healthcare there is risk of data being misused by the cloud computing provider.	53	59	19	22
T19: You believe by using cloud computing in healthcare there is risk of unauthorized data access.	65	62	18	21
T20: You believe by using cloud computing in healthcare there is risk of unauthorised data manipulation i.e. data fraud.	60	51	20	27
T21: You believe by using cloud computing in healthcare there is risk of data exposure to other users of the cloud service.	61	57	19	24
T22: You believe by using cloud computing in healthcare there is risk of losing control over data location.	55	53	21	29
T23: You believe by using cloud computing in healthcare there is risk of data theft via external attacks such as hacking.	68	61	11	16
T24: You believe by using cloud computing in healthcare there is risk of data being accessed by government departments outside of healthcare.	60	55	23	25

Table 3-7 Sample of Response Percentage for Data Security Construct

3.7.2.2 Analysis of Data Security Construct

In the Data Security Figure 3-2, T14 presents the potential readiness of the participants in terms of using cloud computing as a secure channel for transferring medical data across different sites. T15 to T24 present an agreement range of 43 to 68% from the public compared to 44 to 69% of professionals that implied high security concerns, which require mitigation and an approach to eliminate those concerns. There are differences regarding the concerns of professionals and the public in terms of percentages for higher concerns and lower concerns, but it highlights the similar highest concerns, such as data theft, unauthorised data access, data exposure to other users in the cloud, data being misused by the cloud provider and data being accessed by other governments outside of the healthcare domain. In addition, there are three low concern risks at a range of 43% for the public compared to 45% for professionals when using cloud computing in healthcare, such as stolen medical data, security concerns and significant data loss.

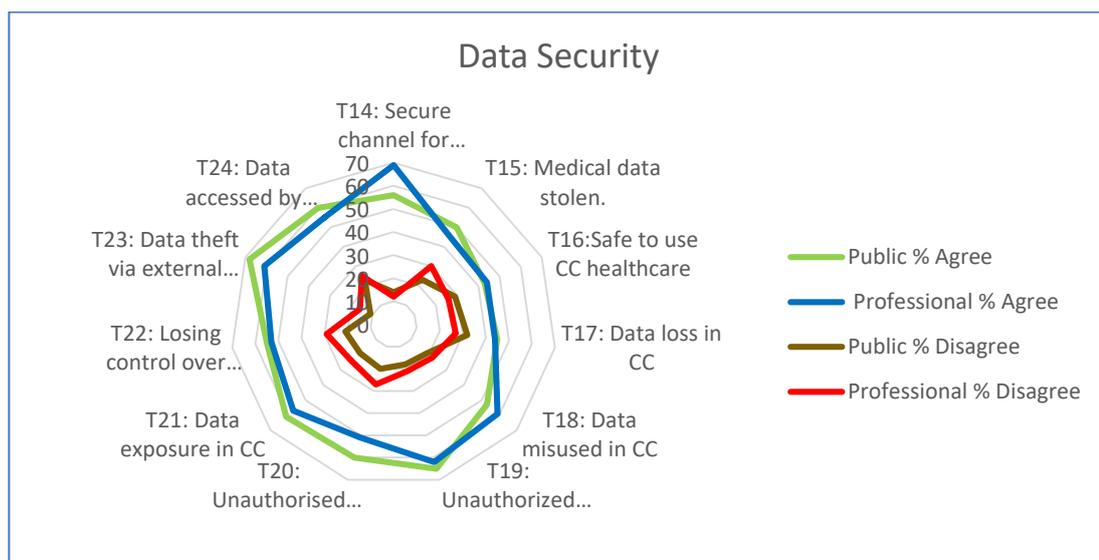


Figure 3-2 Data Security

3.7.2.3 Analysis of Confidentiality, Integrity, Availability Construct

Confidentiality, Integrity and Availability constructs in the radar chart include all questions from the questionnaire apart from T1, T2 and T13. By using Exploratory Factor Analysis (EFA), T1 and T2 generate a new construct, namely Cloud Provider. T13 was dropped because its loading factor was below 0.5. As [Figure 3-3](#) shows, there is a mutual agreement between the public and professionals regarding the various security concerns in using cloud computing in the delivery of healthcare services. It demonstrates the willingness of the healthcare establishment in terms of best practices in relation to Confidentiality, Integrity and Availability (C.I.A) in their current systems. The main role of C.I.A is to help manage data security issues by having the right policies within an organisation. It is clear from [Figure 3-3](#) that there is a broad agreement between professionals (60% to 75%) and the public (63% to 72%) about the security practices that need to be implemented in the healthcare system. However, there is less agreement (13% of the public compared to 20% of professionals) regarding the security measures implemented in healthcare services as well as risk assessments within the current healthcare systems. This implies that there will be issues if they move to the cloud because there will be real risks which need to be addressed professionally. Thus, it is necessary to ensure that a risk assessment plan is conducted within healthcare systems in terms of the data security being implemented. If there is no risk assessment conducted within the healthcare systems, then there will be challenges when moving to cloud-based systems.

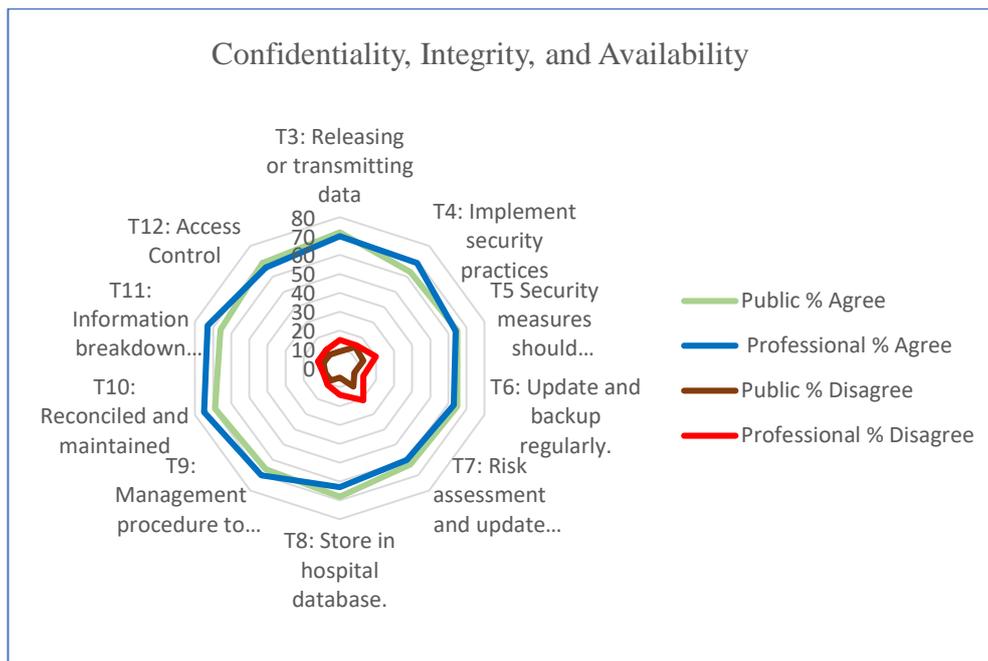


Figure 3-3 Confidentiality, Integrity and Availability

3.7.2.4 Analysis of Complex and Cost Construct

The Complex and Cost Figure 3-4 reveals significant uncertainty among the public and healthcare professionals. For instance, professionals believe that the skills required to use cloud computing in healthcare are too complex for people to use. Hence, it can be seen as a threat which needs a mitigation approach. In contrast, the public perception is that they strongly disagree with the view that learning cloud computing is time consuming; rather they view it as an opportunity to improve healthcare services in Oman. Moreover, T34 presents interesting aspects as professionals are not sure that cloud computing is cost effective when utilized in healthcare services because the cost of maintaining cloud technology is higher than maintaining the current system. Hence, dealing with Complexity and Cost is an important issue that needs to be carefully considered.

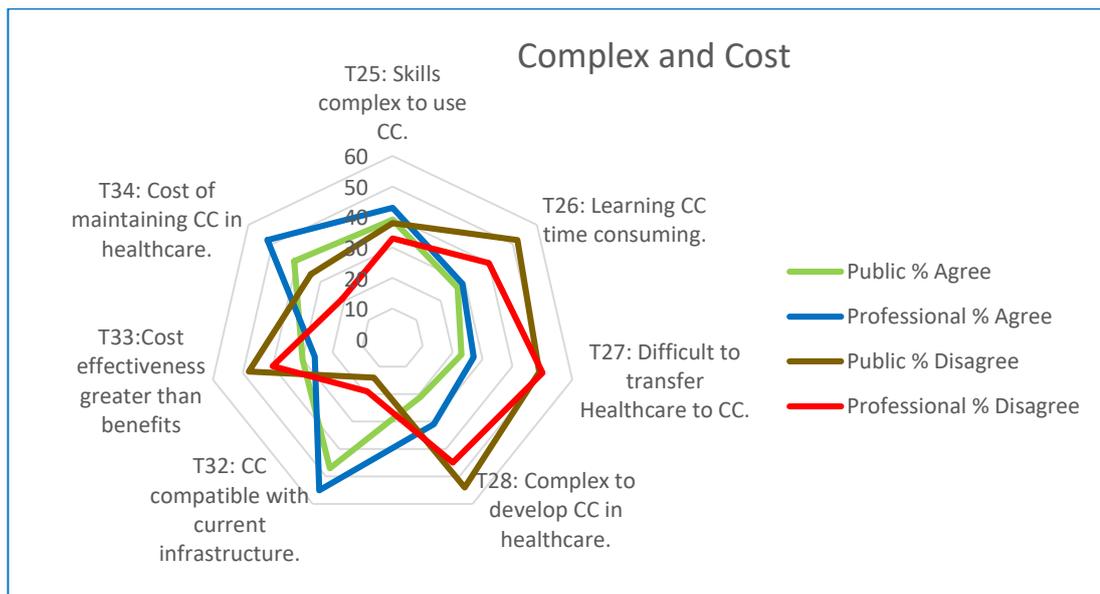


Figure 3-4 Complex & Cost

3.7.2.5 Analysis of Privacy Construct

The Privacy Figure 3-5 shows the perceptions of the public and professionals and their intention to share their details online. Both strongly disagree (84% of the public and 86% of professionals) with sharing their credit card details online as well as sharing their personal details. They are less resistant to share business details but they are ready to share their education details. Hence, it indicates the highest privacy concern regarding the sharing of their credit card details.

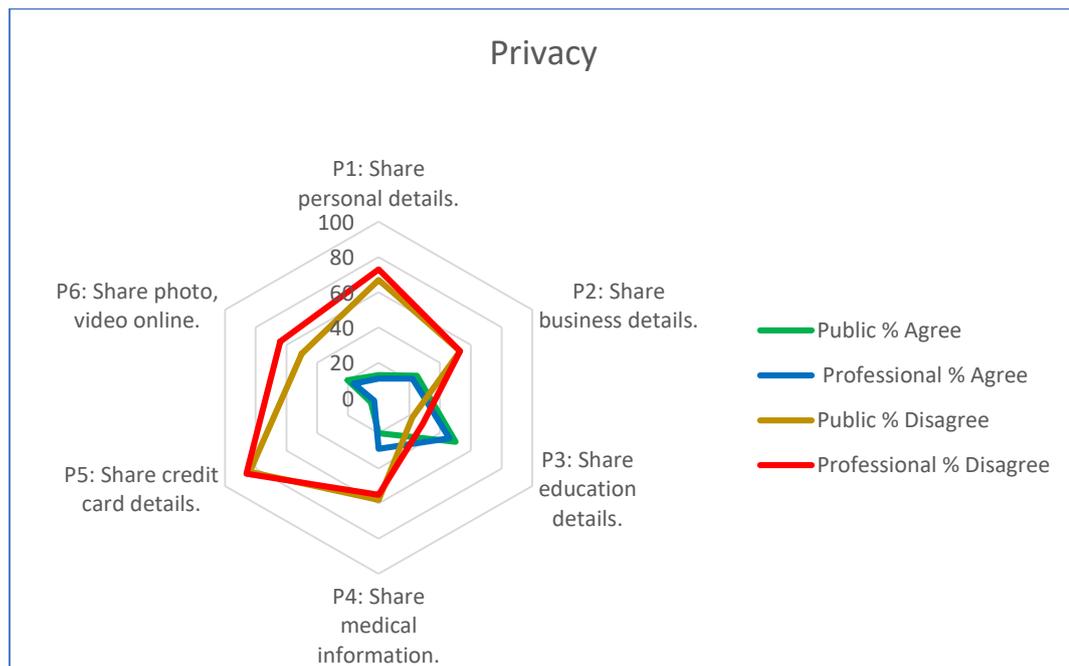


Figure 3-5 Privacy

3.7.2.6 Analysis of Human Construct

The Human Figure 3-6 represents a mutual agreement for the public and healthcare professionals to experiment with new information technologies. In addition, they are enthusiastic about the adoption of cloud computing technology in healthcare services. An agreement range of 36% to 66% for the public and a range of 27% to 58% for the professionals implies that they are ready to accept the changes brought about by the adoption of cloud computing technology in healthcare services.

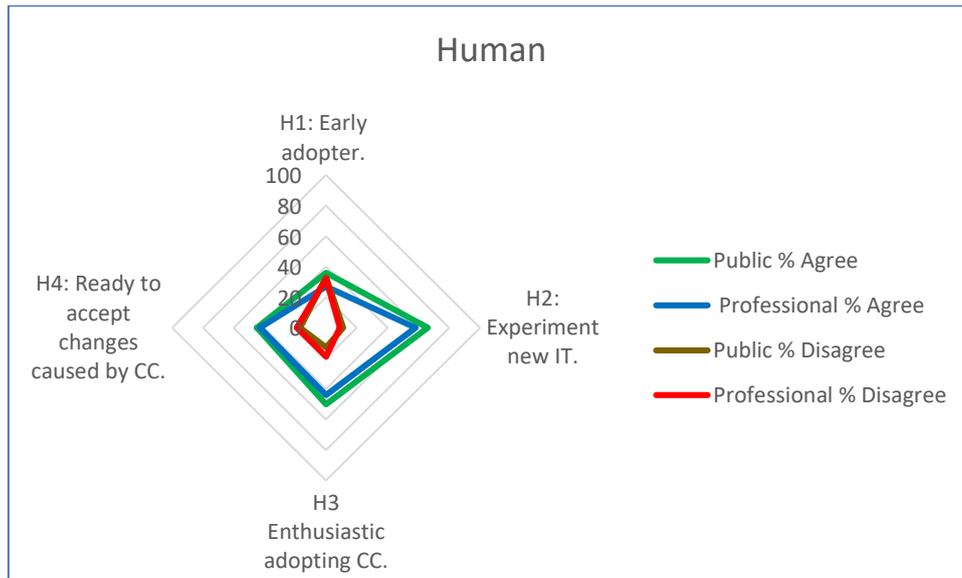


Figure 3-6 Human

3.7.2.7 Analysis of Compatible Construct

As for the Compatibility [Figure 3-7](#), healthcare professionals and the public have a mutual agreement (range of 47% to 60% for the public and 55% to 67% for professionals) that cloud computing is compatible with health care services, values and goals as well as the current infrastructure.

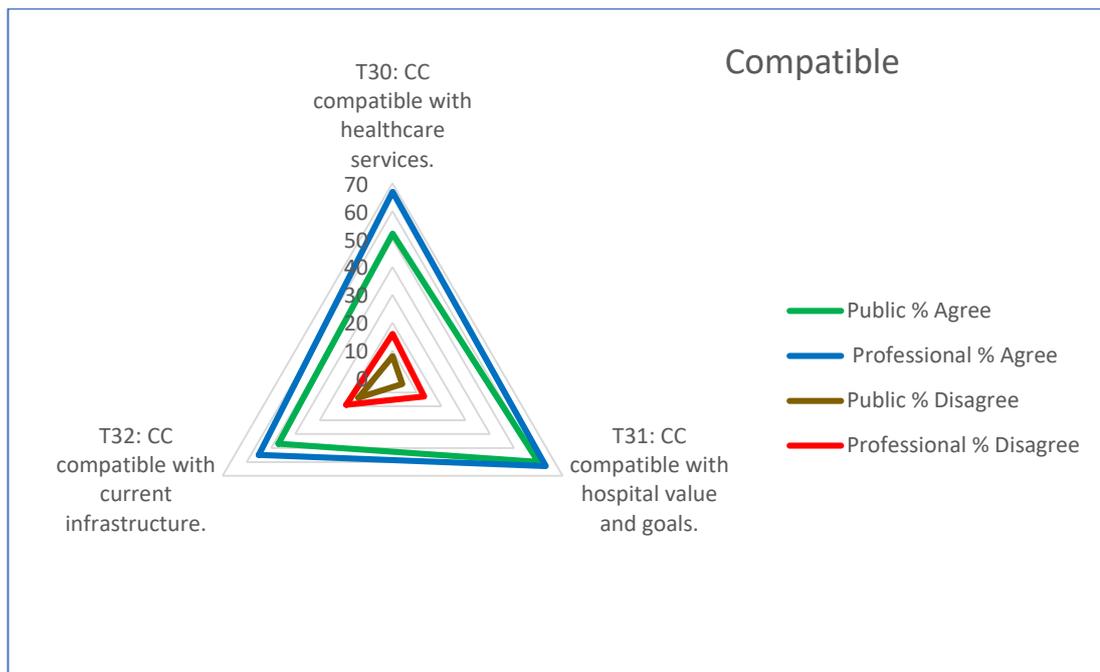


Figure 3-7 Compatible

Radar charts were not created for Internet-based services, business networks and cloud providers as these hold insufficient responses with regards to validity and reliability.

3.7.2.8 Analysis of Relative Advantage Construct (Healthcare Professional)

The Relative Advantage Figure 3-8 reveals healthcare professionals' positive (range of 59% to 73%) attitudes towards cloud computing as a means of improving collaboration and communication, reducing operating costs as well as providing timely access to patient information.

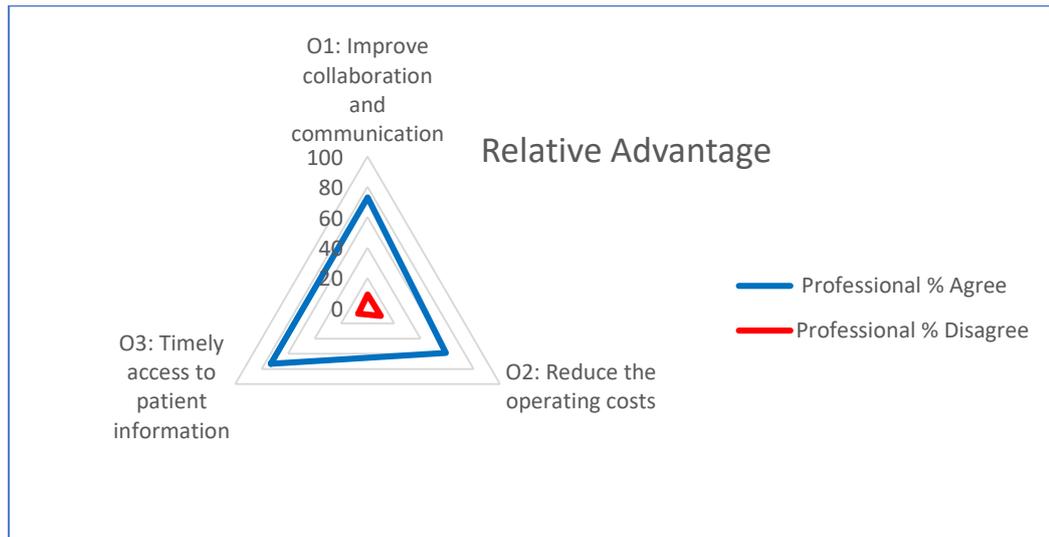


Figure 3-8 Relative Advantage

3.7.2.9 Analysis of Top Management Support Construct (Healthcare Professional)

The Top Management Support [Figure 3-9](#) interprets management support in an agreement range of 47% to 54% in terms of providing sufficient resources and encouraging the development of cloud computing in healthcare. This is because they recognise the benefits of utilizing cloud computing in the delivery of healthcare services.

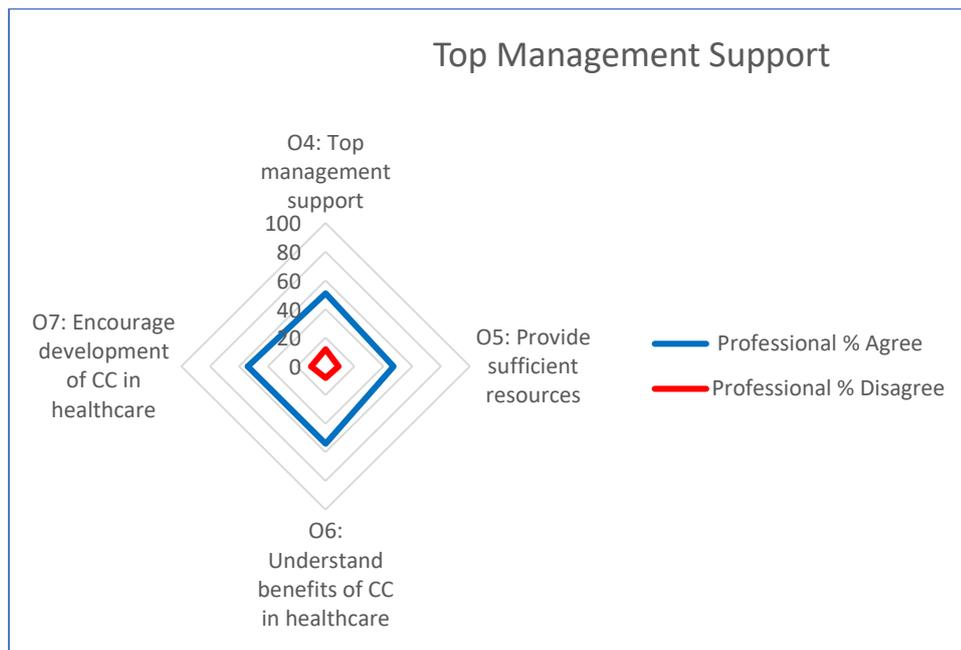


Figure 3-9 Top Management Support

3.7.2.10 Analysis of Adequate Resource Construct (Healthcare Professional)

The Adequate Resource [Figure 3-10](#) explicitly identifies healthcare professionals' positive agreement with a range of 34% to 39% to provide sufficient IT infrastructure, human resources, time and budget to facilitate the development of cloud computing in the delivery of healthcare services. The smaller agreement was in the range of 18% to 25% only.

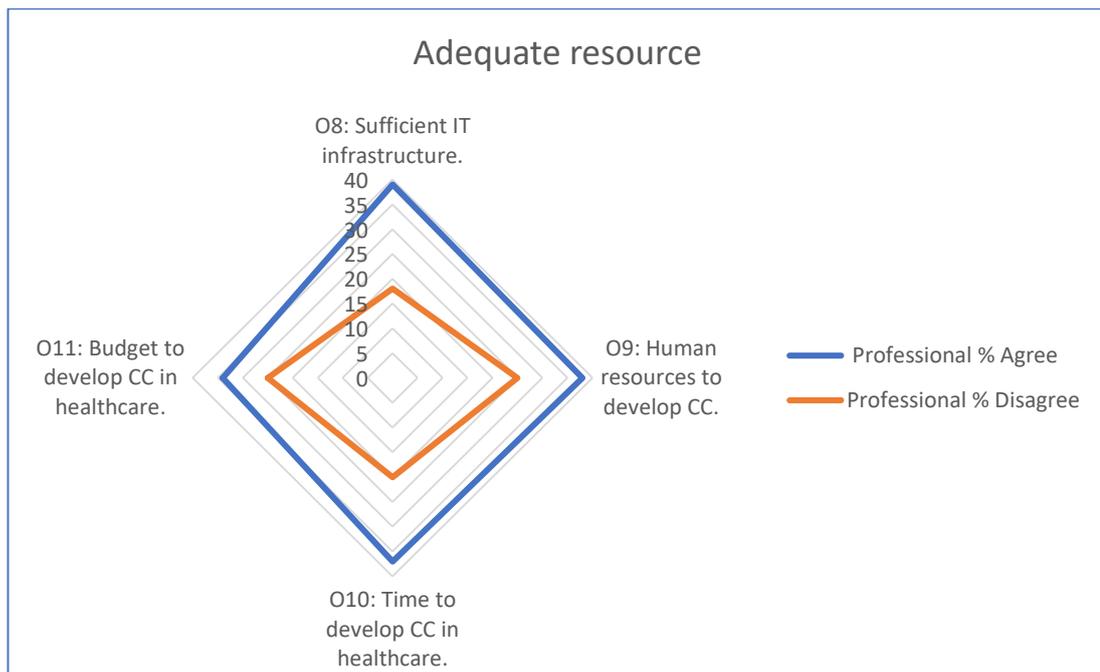


Figure 3-10 Adequate Resource

3.7.2.11 Analysis of Benefit Construct (Healthcare Professional)

The Benefit Figure 3-11 explains, in depth, the motivation for professionals' positive agreement for utilizing cloud computing in the delivery of healthcare services. The most important benefits scored almost 73% in terms of reducing the time for doctors to access patient treatment plans and increasing health research and collaboration. The second motivation was that using cloud computing can reduce duplicate patient tests and improve the hospital's image and expertise (an average of 70%). In addition, it can improve internal efficiency and service quality in healthcare and reliability of IT resources. The only percentage that falls to 60% indicates that they are uncertain how technology can improve the relations between the hospital and patient.

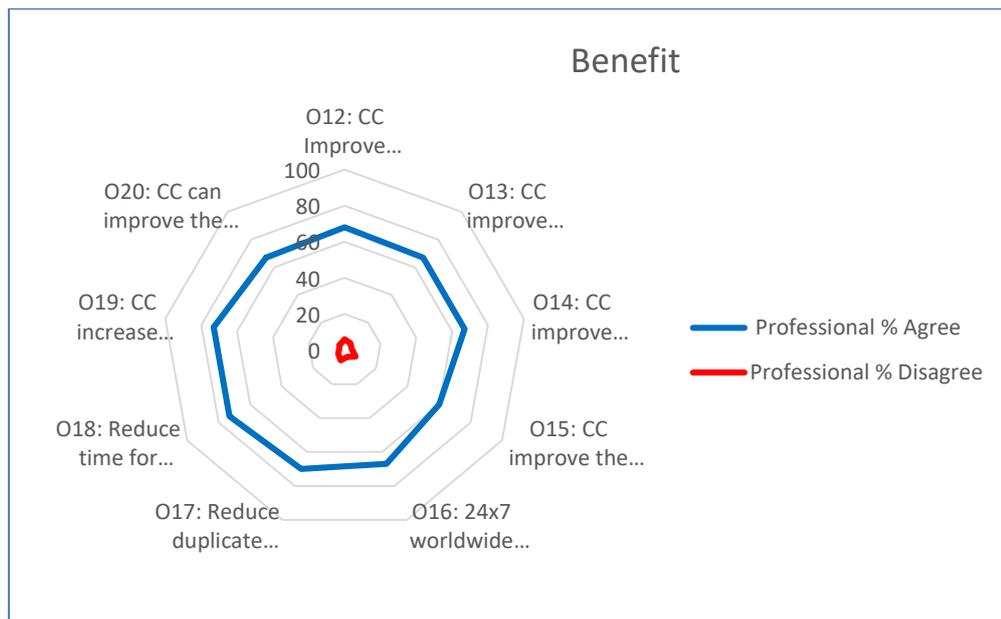


Figure 3-11 Benefit

3.7.2.12 Analysis of Environmental Construct (Healthcare Professional)

The Environmental Construct [Figure 3-12](#) shows broad agreement with at least 60% regarding the need for training courses in using cloud computing in healthcare to be provided by the government as well as the need to develop electronic medical records using cloud computing. On the other hand, almost 57% believe that high quality courses should be provided by the hospital and not the government.

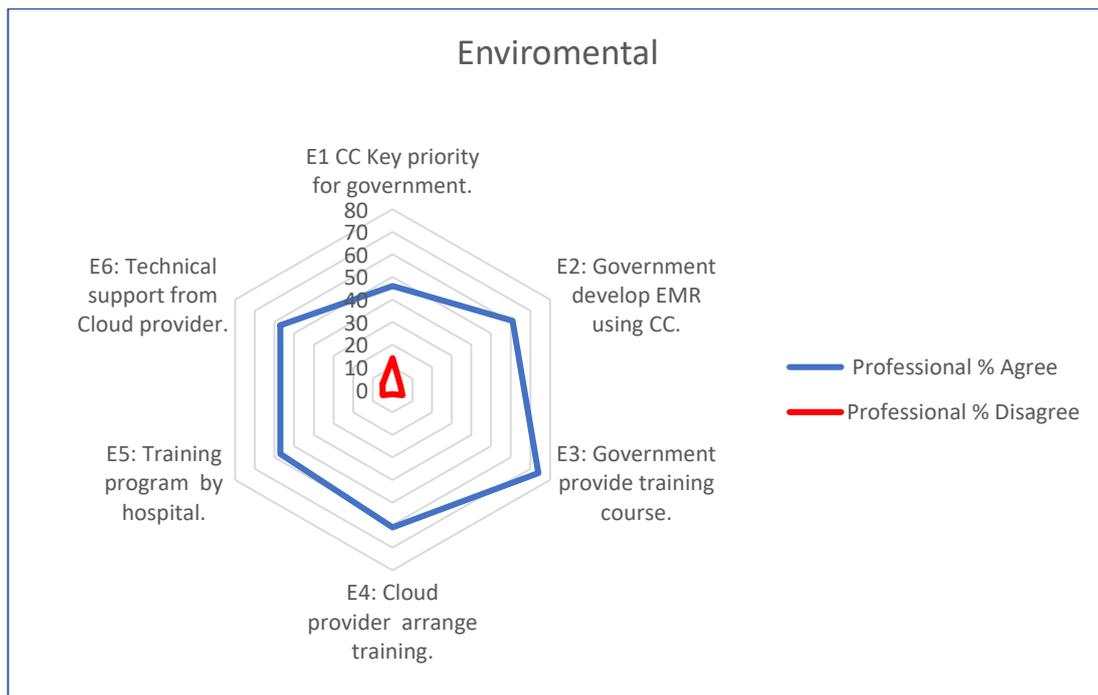


Figure 3-12 Environmental

3.8 Research Validation

The findings from the preliminary interviews and questionnaires illustrate the perceptions of risk within the Omani context. According to the interviews conducted, the main barriers for utilizing cloud computing in healthcare services are the Confidentiality, Integrity and Availability of patients' medical records, as stated by CC01 and CC02. In addition, the questionnaires findings highlighted the key concerns regarding Data Security as well as Confidentiality, Integrity, Availability, Complex and Cost and Privacy as the highest concerns for both the public and healthcare professionals. The findings in this study echoed those of Lian et al. (2014) related to understanding the critical factors affecting Taiwan Hospital in adopting cloud computing in healthcare services; it was found that the five most critical factors were data security, perceived technical competence, cost, senior manager support, and complexity.

To validate the questionnaire findings, an interview was arranged with H.Dr. Ali Talib Al Hinai, Undersecretary for Planning Affairs in Ministry of Health where he pointed

out that MoH used cloud computing as infrastructure as a service by hosting the ministry's website in the cloud. The online system provided various services to patients but in different phases. For example, services included applying for tender or discharged summary and allowing patients to book and cancel appointments. However, a patient cannot view his/her medical record online for security concerns. He strongly emphasised the need for a high security mechanism to release patient records: “...*There is a need for organized security mechanism which permits viewing patient record online. In UK it is not allowed for patient to view their medical records online. In U.S it is not allowed too but in Canada patient can have access to his medical records online*”. In addition, he highlighted the importance of rules and regulations in each country which control privacy regulations when it comes to disclosure of patient records: “...*Each country differs than other country according to rules and regulations. With us here in Oman, it is not allowed to view patient medical records except for authorized people*”.

In addition, H.Dr. Ali Al Hinai pointed out that access control is restricted among hospital staff according to their role and job responsibilities: “*Clinical pharmacy cannot view all patient records, and administrator staff cannot view patient records. Each staff according to their roles and responsibilities. The only person can view patient medical record is the consultant if the patient under his name of treatment people. He can view the treatment plan for the patient, any surgical conducted and medication. However, the consultant cannot view the administrative work such as budget for the hospital or any financial issues*”.

A hypothetical scenario was provided of a woman from Germany going to the U.S to attend a conference but her taxi was hit by another car. She was unconscious in the emergency unit. The doctors prescribe a medicine she is allergic to. Luckily, the doctors are able to access her smartphone, which indicates her medical history; the doctors changed the medicine which could have killed her.

H.Dr. Ali, comments, “*there is a different to put medical records online or to put it in cloud. The risk is too high in cloud. Using Al Shifa system there is an internal server*

in ministry of health. The risk will be internal but when you put it in cloud there will be external risks from hackers from anywhere. It is fine to provide services online to book or cancel appointment even if it hacked by someone it is not major concerns. But having patient file is top secret. If you put patient file in cloud there is high risk of it being hacked. The cloud provides good services except for patient file”.

He also mentions Al Shifa software: *“Al Shifa provide different services for citizens and residents excluding patient medical records. Currently the citizens and residents can use their ID card to give hospital or health centre authority to view his medical record when he need treatment. At later stage there will be central database which unify patient file in one place”.* He refers to one of the future projects discussed in section 3.2 (*Consolidating and Standardizing the Database of Diagnosis, Radiology and Laboratory Tests (CSDDRLT)*) within MoH to unify the different databases and standardise the identification codes to facilitate seamless communication between healthcare providers with the aim of reducing misinterpretations.

H.Dr. Ali AlHinai was asked to rank the main security concerns regarding technology factors according to their importance when utilising cloud computing services in healthcare in the future. The first were related to privacy and data security as he indicated. Second, he prioritised internet-based services followed by complexity and cost. The third concern was confidentiality, integrity and availability of patient medical records followed by provider control and business application and social network.

3.9 Reflection on Results

The results were considered from the preliminary interviews conducted with seven different stakeholders, the questionnaire feedback from 150 healthcare professionals, 400 patients’ perceptions, Radar Chart and the interview with the Undersecretary for Planning Affairs in MoH. Several important points were identified.

The questions statements for public and healthcare professional's questionnaires were adopted from Lian et al., (2014) which investigated the critical factors that affected the decision to adopt cloud computing technology in a Taiwan hospital. Wijaya et al. (2014) discussed Indonesian awareness of health records stored in cloud computing and it was interesting to find out the responses based on the user's IT background and those who do not have the IT background through Yes/No questions. In addition, the Internet based services and privacy questions statements were adopted. Since technical solution alone was not sufficient, Singh et al., (2014) and Chang et al., (2007) investigated the organisational factors which can affect information security. The questions statement for top-management-support, adequate resources and government policy was used in Lian et al. (2014) research. The reliability and validity of questions were checked through factor loading and Cronbach's Alpha. As a result of this process, some of the questions were dropped.

The results demonstrated readiness to utilize cloud computing as a service in healthcare but showed an awareness of a range of threats that will require a mitigation approach to address. In addition, the results focused on the need to plan and implement security measures as well as conducting risk assessments to avoid any loss of information. Having the risk assessment implemented on a regular basis will help healthcare establishments to mitigate risks when moving to the cloud-based system. Moreover, Complexity and Cost concerns illustrated an important aspect to deal with the skills and time limits required to use cloud computing and learn how to benefit from cloud services within healthcare respectively. In addition, the findings highlighted that cloud is viewed by stakeholders as cost effective when maintaining it compared to the current system.

The Data Security radar chart and the Confidentiality, Integrity and Availability chart clearly shows that the public and healthcare professionals are in mutual agreement about the security issues on what to agree and disagree on. A paradox arises between 'privacy and security' and 'confidentiality, integrity and availability'. In e-healthcare, conditions of confidentiality, integrity, availability, accountability, non-repudiation

and others need to be met. Without this privacy, it will not be possible to gain patient trust in the system. On the other hand, sharing medical records between healthcare practitioners requires access to patient records online. Therefore, a distinction is made between those who are allowed to access health records and those who are not (Sahi et al., 2018).

In contrast, it is hard to identify stakeholders' perceptions in the Complex and Cost chart as it presents high uncertainty between what they agree and disagree on. Although the percentages are different, the shapes are similar among the agreements and disagreements. The professionals perceived learning cloud computing as being time-consuming. In addition, in T34, professionals observed maintaining cloud computing as being costly compared to 20 percent less among the public. Similarly, the Privacy chart shows a similar proportion regarding the agreement and disagreement issues among the public and healthcare professionals. It was surprising to see that the public and healthcare professionals are less resistant to sharing their medical records compared to their credit card details. They both agree to sharing their education details online.

Looking at the Human chart and Compatibility chart, there is a clear separation between agreement and disagreement, which indicates that the public and professionals agree on the same concerns. Therefore, based on the radar chart, there is a need for security measures to be considered as a high priority. There are different security threats, which require a methodology framework to help understanding how to address management threats, such as human readiness and senior management support.

Although Information Technology Authority (ITA) follows the International standard of Information Security Management Systems (ISO 27000) security guidelines, the undersecretary did not approve hosting the patient medical records online, even if the hosting cloud is within Oman, due to security risk concerns.

The statistical information obtained from questionnaires presents a wide range of factors that affect cloud-computing adoption. It provides an in-depth study of the perception of risks in healthcare when adopting the cloud. This is important as it provides the basis for other anticipated risks in the area that will require further investigation. Those factors can form the basis for other research within different fields, such as SMEs, Telecommunication and Education.

Due to time constraints, this thesis will investigate the security risks as it is the main concern identified from the preliminary interviews with stakeholders, questionnaires and the interview with the Undersecretary. Therefore, this thesis will focus on developing a risk assessment methodology that can address security threats. Other types of risks, such as managerial risks, top management support and employee readiness, can be addressed in future work.

As a recommendation for the Omani government, this research highlights the need for training and awareness workshops for citizens and residents in order to raise awareness of security threats when utilising cloud computing services. Increasing the awareness level of security threats may reduce the security risks as individuals would be cautious of data breaches of their data. In addition, the cloud provider needs to be certified by the local government to gain customer trust through empowering the service level agreement and security service level agreement.

3.10 Conclusion

To understand the current situation in Oman regarding cloud computing usage, a mixed research methodology approach was used. Six stages: research problem, research hypothesis, research questions, interview, questionnaire and validation were implemented. First, to identify the research problem, domain analysis on cloud computing background was carefully studied. The researcher was able to gain deep understanding of cloud computing benefits as well as anticipating various risks when

utilizing it in healthcare. Second, preliminary interviews helped to understand the current situation in Oman and enhanced the need to administer questionnaires for the public and healthcare professionals to understand their perceptions of security risks (Data Security, Confidentiality, Integrity, Availability, Complexity, Cost, Privacy and Compatibility) when utilizing cloud computing in the delivery of healthcare services. The comprehensive statistical information obtained from these questionnaires provided a basis for further investigation within different industries, such as SMEs, Telecommunication and Education

In order to validate the results obtained, an interview was conducted with H.Dr. Ali Talib Al Hinai, Undersecretary for Planning Affairs in Ministry of Health. The outcome supported the findings of the questionnaires and guaranteed the validity and accuracy of the respondents' responses. Also, the interviewee highlighted the need for an effective security risk assessment methodology to overcome the identified security concerns. Hence, there is the need to have an effective risk framework methodology to address those risks. Although Information Technology Authority (ITA) follows International Standard for ISO 27000 to identify many security risks, it does not specifically address the healthcare domain.

There is a need for an organisation to have an effective risk management approach to manage risks. If the organisation does not have a clear understanding of where risks are encountered, then there might be a problem related to not having awareness of risks. Organisations adopt risk management standards which provide assurance that the organisations are following those standards which provide techniques and procedures to manage the risks.

Chapter 4 provides a review of the standards, methods and tools that are used to manage risks to understand strengths and limitations to move forward and provide a method which provides a shared understanding of risks.

Although there are international standards which help manage risks by providing a generic framework, the key limitation is that the standards themselves do not explore in sufficient detail how to visualise those risks.

The next chapter will also discuss Business process modelling and will review methods that have been used to help visualise risks.

4 Chapter 4: Managing Information Security in Healthcare

4.1 Introduction

This chapter will present managing information security as the research problem. It will discuss the business context through ISO/IEC 38500 for Corporate Governance of Information Technology and Risk Management standard (ISO 31000) as it is widely used in managing risks. In addition, Managing Information Security (ISO 27000) and Information Security Risk Management (ISO 27005) will be discussed to understand the mechanism in managing information security risks. A critical analysis of the tools and techniques for each standard will be presented. Tools and techniques for managing risks in healthcare, such as Risk Register (RR), Operational Critical Threat and Vulnerability (OCTAVE) and Failure Modes and Effect Analysis (FMEA), will be explored. An analysis of those techniques based on the ISO 27005 stages was performed to identify their limitations as well as the most appropriate tool to use. The Risk Register was found to be the most appropriate. It is also widely used in healthcare despite the difficulty to visualise risks in a large risk register document.

In addition, a review of Information Security will be presented as a major concern to address. The role of process modelling prospected in risk management framework will be considered.

Business Process Modeling (BPM) is a widely used modelling technique, especially in healthcare, and will be used to model information security in healthcare processes. It was ascertained that to better understand the risks, it would be necessary to enhance the communication of risks in process modelling. To identify a solution for the problem, Risk Register and Business Process Model were combined.

There is a need for an effective risk management approach that manages risks by providing visibility and shared understanding of risk. In this thesis, it is proposed that combining the Risk Register with Business Process Modeling (BPM) can be more effective in communicating the information security risks which will be addressed in

Chapter 5. The remainder of this chapter will explore BPM and highlight how BPM has been used to model security.

4.2 Corporate Governance of Information Technology (ISO 38500)

ISO/IEC 38500 is an international standard for Corporate governance of information technology published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (Mayer et al., 2015; Mahy et al., 2016). The objective of ISO/IEC 38500:2015 is to provide guiding principles for members of governing bodies of organizations (which can comprise owners, directors, partners, executive managers, or similar) on the effective, efficient, and acceptable use of information technology (IT) within their organizations (Mayer et al., 2015; Mahy et al., 2016). It also provides guidance to those advising, informing, or assisting governing bodies (Mayer et al., 2015). The governance of IT is considered as a subset of organizational governance (or corporate governance). ISO/IEC 38500:2015 is applicable to all types of organizations (i.e. public and private companies, government entities, not-for-profit organizations), whatever their size and regardless of the extent of their use of IT (Mayer et al., 2015).

The primary advantage of the ISO/IEC 38500:2008 IT governance framework is its assurance that accountability is clearly assigned for all IT risks and activities. This specifically includes assigning and monitoring IT security responsibilities, strategies and behaviours so that appropriate measures and mechanisms are established for reporting and responding in relation to the current and planned use of IT such as meeting the latest data protection requirements for encryption of all portable devices such as laptops and memory sticks used to store and transmit personal data (Van Haren Publishing, 2018).

However, there are two constraints of the ISO/IEC 38500:2008. 1) Outsourcing: some requirements are so specific to the managers of IT. That is these requirements cannot be imposed on the managers of the company if their IT is outsourced. In cases such as these,

the requirements will need to be secured in the contract with the supplier of IT services. 2) Applying the standard in isolation: ISO 38500 is not ‘one size fits all’. It does not replace COBIT, ITIL, or other standards or frameworks, but rather it complements them by providing a demand-side-of-IT-use focus (Van Haren Publishing, 2018).

The main tasks to be followed by IT governing bodies, represented in Figure 4-1, are: 1) Evaluating the current and future use of IT. 2) Directing preparation and implementation of strategies and policies to ensure that the use of IT meets the business objectives. 3) Monitoring conformance to policies, and performance against the strategies (Mayer et al., 2015).

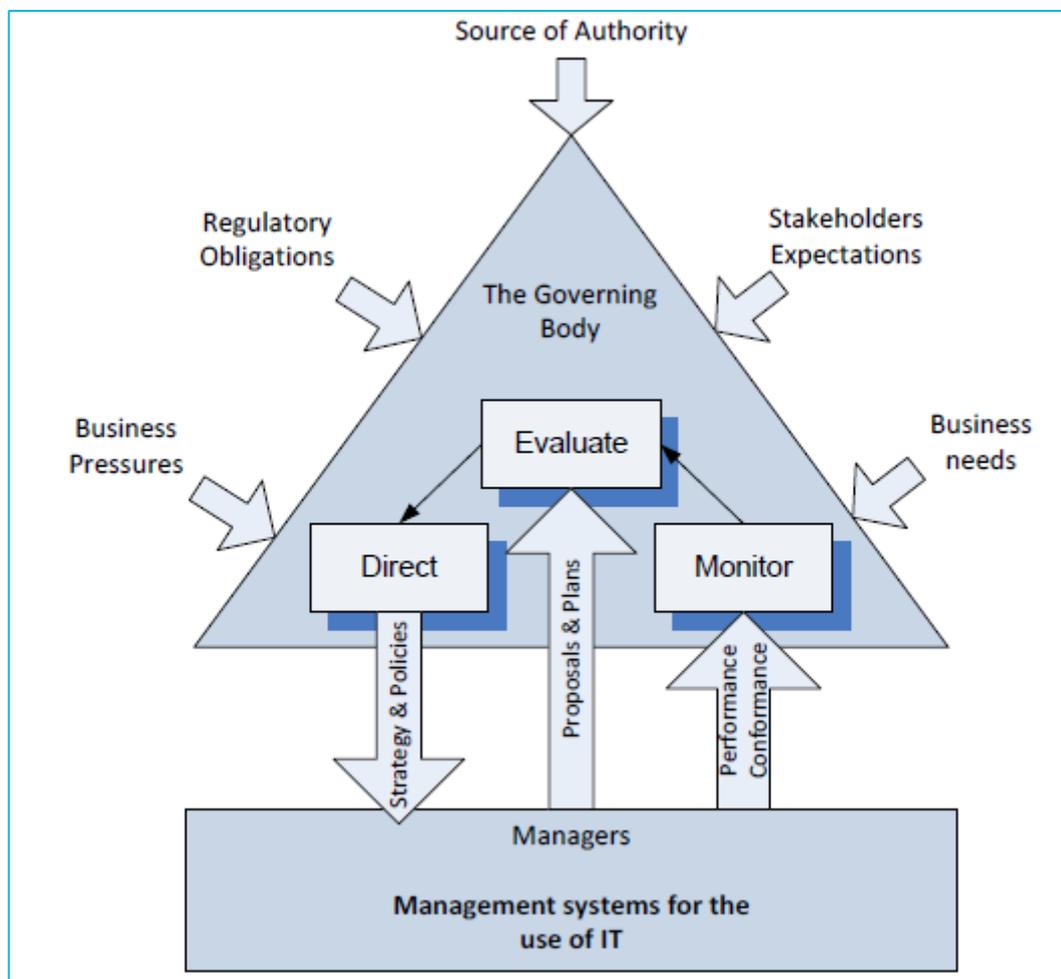


Figure 4-1 Model for Governance of IT
Source: (Mayer et al., 2015)

As ISO 38500 covers governance of information technology which includes assigning and monitoring IT responsibilities, there is a need for a system that focuses on managing

risks. ISO 31000 for organisational risk management was introduced for organisational risk management, which will be explained further in the next section.

4.3 Risk Management (ISO 31000)

To understand the mechanism of managing the identified risks, risk management standards were carefully studied. Risk management standards set out a particular set of strategic processes that start with the general objectives and aims of an organisation. They help to identify risks and promote the mitigation of risks through the best practice. Risk management standards are a guide to help ensure that risk management is carried out consistently. Standards usually include guidelines and examples to facilitate the compliance of organisations. They have been designed to facilitate the implementation of risk management processes. These standards contribute to providing an international consensus on how to deal with specific risks, and they offer advice on how to address them according to the best practices in the field. Risk management standards help organisations to implement strategies that are tried, tested, and proven to work.

Risk management is a fundamental concern in any organisation to manage uncertainty by identifying and understanding risk and modifying it where necessary. Some researchers consider risk management as a tool to avoid threats and identify opportunities (Spikin, 2013). Lubka (2002) indicated that risk management acts as a way of helping the company to achieve its goals. The ISO 31000 Risk Management Standard has been widely used to help organisations to systematically and comprehensively manage diverse types of risk by offering a universal framework, “to assist the organisation to integrate risk management into its overall management system” (ISO, 2009a, p. 9). Therefore, the ISO 31000 standard provides guidance for making risk management central to the success of an organisation and for making it an integral part of critical processes such as planning, management and governance (Gjerdrum and Peter, 2011). Organizations are encouraged to adopt management models that consider the increasing diversity and complexity of risks (Lalonde and Boiral, 2012).

According to the ISO 31000 standard, each organisation should identify all the risks concerning the organisation's objectives that are designed to achieve its mission. One of

the primary goals set out by the ISO 31000 standard is to continually improve risk management in organisations based on a generic model that is intended to adapt to a wide variety of risks (Lalonde and Boiral, 2012). Woody et al. (2006) identified risk management as the ongoing process involved in identifying, assessing and judging risks, taking actions to mitigate or anticipate them and monitoring and reviewing processes. Thus, performing risk management is considered as a vital tool to continuously observe damages and identify opportunities.

Lalonde and Boiral (2012) suggest that risk management should be seen as a practice-based approach; a strategy that managers *do* and not a strategy that managers *have*. In this regard, managers must question their assumptions regarding the implementation of such a standard taking into account the specificities of their internal and external organisational environment and remaining cautious in its monitoring. Also, Gordon et al. (2009) pointed out that instead of looking at risk management from a silo-based perspective, the trend is to take a holistic view of risk management. Hence, each organisation in various sectors (i.e. Health, Telecommunication, Transportation and Banks) has to design its risk management framework that includes practices, processes and resources that enable risk management.

According to ISO 31000, risk management consists of three steps: (i) identification, (ii) assessment, and (iii) prioritisation of risks, that aims to minimise, monitor and control the probability and impact of unfortunate events (Lam et al., 2015). ISO 31000 risk management activities are based on the Plan-Do-Check-Act model. By using the PDCA model, the *Plan* phase will establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results under an organisation's overall strategies and goals. The *Do* phase will implement and operate the ISMS policy, controls, processes and procedures. The *Check* phase will assess and measure process performance against ISMS policy, objectives and practical experience and report the results to management for review. Finally, the *Act* phase will maintain and improve the ISMS by taking corrective and preventive actions based on the results of the internal ISMS audit and management review or other relevant information to achieve continual improvement of the ISMS.

The ISO 31000 provides guidelines but does not suggest specific procedures or metrics by which an entity should apply and/or measure risk management (Lalonde & Boiral, 2012; Spink et al., 2016). Therefore, a methodology framework is needed to manage various types of risks within an organisation.

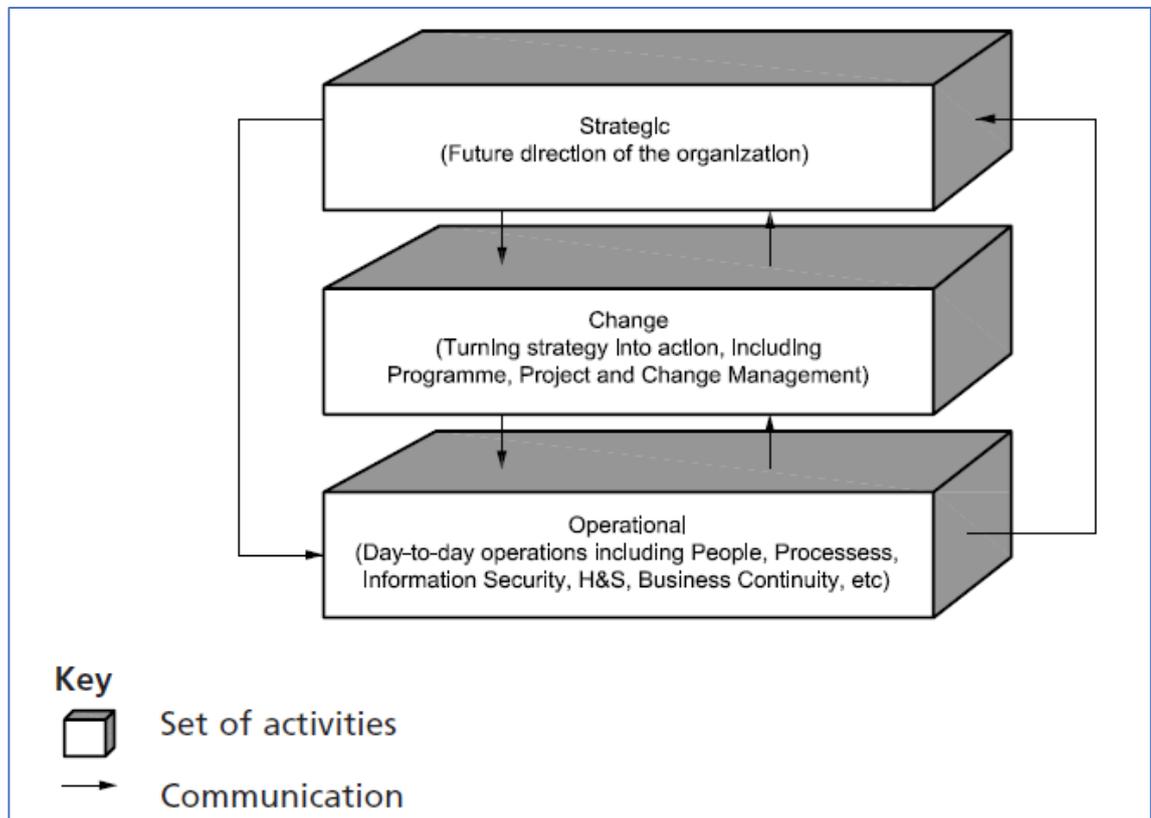


Figure 4-2 Risk Management Perspectives
Source: BS ISO 31100:2011

ISO 31000 categorises activities into three risk management perspectives (Figure 4-2) which are strategic, change and operational. The strategic aspects focus on the future direction of the organisation. Strategic risk is a process performed by senior management for identifying, assessing and managing risks and uncertainties. As an organisation attempts to achieve its strategic objectives, both internal and external events can create risks that prevent an organisation from achieving its objectives (Taylor, 2013). The future plan could be included in the strategic objectives' level where activities to understand risks associated with entering new services are expanding the existing services through enhancements and mergers, enhancing infrastructure are highlighted (Taylor, 2013).

As for Change aspects, they focus on the process of turning a strategy into an action including projects and change management. Change management is an important part of every successful project. Project risk management focuses on opportunities and threats within a project. Risks associated with change are an outcome that causes a change whether that change has a benefit or an adverse effect on the running of a business. Each change made is a risk .

Operational aspects include day-to-day operations including people, processes and information security. Operational risk management is defined as a continual cyclic process which includes risk assessment, risk decision-making, and implementation of risk controls. These should result in acceptance, mitigation, or avoidance of risk (Taylor, 2013).

ISO 31000 focuses on a system for managing organisational risks by providing guidelines for identifying the internal and external context. It provides a framework for managing all kinds of strategic change and operational risks on a company-wide level. However, ISO 31000 does not offer any specific advice about information security risk. Therefore, ISO 27000 is necessary for managing information security risks. ISO 31000 and ISO 27000 are compliant with each other. ISO 27000 family of international standards focuses on managing information risk. In addition, ISO 27005 is a standard that provides guidelines for information security risk assessment and treatment. It provides the knowledge to identify assets, threats and vulnerabilities to assess the consequences and probability and to calculate risk. Also, it is completely compliant with ISO 31000. ISO 27000 and ISO 27005 will be explained further in the next section.

4.4 Managing Information Security Risk (ISO 27000)

Managing information security risks plays a significant part within any organisation or industry which needs to be managed professionally. The ISO/IEC 27000 series of standards are internationally recognised and broadly implemented Information Security (InfoSec) standards. The series were established by a joint committee of the International Organisation for Standardisation (ISO) and the International Electronic Commission

(IEC). They cover InfoSec management, InfoSec risk management, implementation of InfoSec Management Systems (ISMS), measurements and metrics of ISMS.

In 2000, ISO adopted BS7799, which represent the standards that were published by the British Standard Institute in 1995 under the name ISO/IEC 17799. BS7799 was grounded on the Code of Practice for Information Security Management, which was established by the Department of Trade and Industry and was closely linked with leading UK organisations. In 2007, ISO/IEC 17799 was combined in the ISO/IEC 27000 series as the ISO/IEC 27002. The ISO 27001 contains the specifications for an information security management system (ISMS). The ISO 27002 outlines the code of practice for information security control for reducing risks; ISO 27003 details information on security management system implementation guidance; ISO 27004 covers information security system management measurement. The ISO 27005, however, presents a methodology independent ISO standard for information security risk management.

According to ISO 27000, information security consists of *“the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation's information security to achieve business objectives. It is based upon a risk assessment and the organisation's risk acceptance levels designed to treat and manage risks effectively. Analysing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information assets, as required, contributes to the successful implementation of an ISMS”* (ISO 27000: 2016).

According to Humphreys (2008), ISO/IEC 27001 and ISO/IEC 27002 controls provide comprehensive coverage of the organisational requirements for managing risk across the business involving people, information, processes, services, IT and physical assets. The origins of the ISO27001 (BS ISO, 2005a) and 27002 (BS ISO, 2005b) standards were informed by the work of the UK DTI and BSI (Gillies, 2011). The ISO27001 standard provides a model for *“establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS)”* (ISO, 2005a; Gillies, 2011). The ISO27000 series of standards have only been slowly adopted.

Evidence regarding the barriers to adoption suggests that the approach is overly complicated and costly for many small organisations (Gillies, 2011). Risk management is a significant element which an organisation needs to perform to guard its assets. If an organisation does not know the risks it faces, it will not be able to implement adequate protection. Humphreys (2007) emphasised that assessing risks includes identifying the assets. Once the risks have been determined, a risk register should be created to record these risks according to their severity as well as details of the risk type, the estimated impact and other information that will be useful to build up a risk profile for the organisation (Humphreys, 2008).

Wright (1999) indicated that risk management is a process of establishing and maintaining information security within an organisation. The measure of risk assessment through information security risk assessment is considered effective when an organisation can respond appropriately and cost effectively to protect information. In 2001, Reid and Floyd devised the “risk analysis flow chart” and emphasised that an organisation should assess the threats and vulnerabilities of its information assets. The primary objective of any organisational control is to lower the risk to an acceptable level. Hence, joining risk assessment and risk control places information security risk at an acceptable level.

An information security risk evaluation is part of an organisation's activities for managing information security risks. Alberts et al. (2003) pointed out that during the application of the Operational Critical Threat and Vulnerability (OCTAVE) approach, an analysis team identifies the organisation's information security risks, analyses the risks to determine priorities and plans the needed improvement by developing a protection strategy for both the organisational development and risk mitigation to reduce the risk of the organisation's critical assets. By using the OCTAVE approach, an organisation makes information protection decisions based on the expected risks of the organisation's confidentiality, integrity and availability of vital information-related assets (Alberts et al., 2003). OCTAVE is an evaluation activity, not a continuous process. Thus, it has a defined beginning and end.

According to Rukh and Malik (2017), ISO 27001 standard framework was applied to resource management in a real-world organisation. The results of this mapping show that

all clauses of ISO 27001 standard, except Clause 6, are fully applicable to resource management. Clause 6 is partially relevant due to information security-specific controls. These results suggest that an organisation can use ISO 27001 standard framework to improve performance and efficiency in other management areas if needed and to mature their process (Rukh and Malik, 2017).

4.5 Information Security Risk Management (ISO 27005)

Information Security Risk Management (ISO27005) defines risk management as “*coordinated activities to direct and control an organisation with regard to risk*” (p. 8) and describes the risk management process as ‘*a continuous process of systematically identifying, analysing, treating, and monitoring risk throughout the life cycle of a product or service*’ (p. 8) (Alshaikh, 2014). ISO 27005 provides guidelines for an organisation to support the requirements of information security management (ISMS) according to ISO 27001. ISO 27005 has been created to support ISO 27001 by providing more details on the concepts and methods behind the risk assessment process. It also provides four options for risk treatment namely: accept/retain the risk, avoid the risk by modifying or avoiding the planned activity that causes the risk, transfer the risk by insurance or by contracting out the risk, and reduce the risk by implementing a system of internal controls (Humphreys, 2008). However, it does not provide any particular method for information security risk management. It depends on the organisation to identify their approach to risk management according to their scope of ISMS. ISO 27005 applies to managers and staff involved with information security risk management within an organisation. As Stoneburner et al. (2002) and Whitman & Mattord (2010) emphasised, information security managers have the crucial responsibility for managing information security risk within an organisation by employing risk management practices (Alshaikh, 2014).

According to a study conducted by Lisiak-Felicka and Szmit (2014), the main reasons for not implementing ISMS are lack of funds, lack of sufficient knowledge and lack of time. To achieve the successful implementation of ISMS, it is crucial to continue raising employees’ awareness at all levels of the organisation and facilitate their respective practical preparation (Lisiak-Felicka and Szmit, 2014).

Risk Management Standard (ISO 31000) and Information Security Risk Management (ISO 27005) complement each other. While ISO 31000 represents the organisational structure of the risk management process, the ISO 27005 is focused on information security risk management process, which is consisting of: context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation, and risk monitoring and review. Figure 4-3 represents an illustration of the information security risk management process.

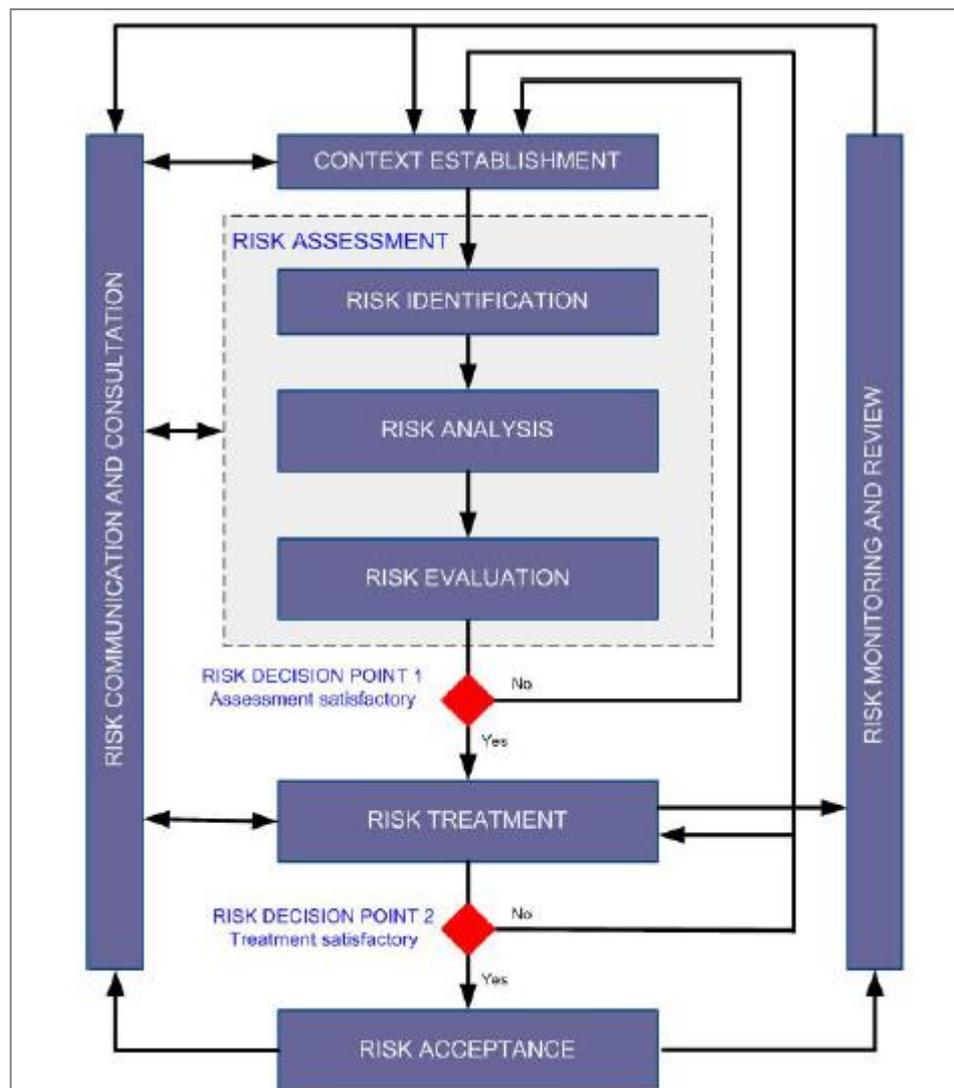


Figure 4-3 Illustration of Information Security Risk Management Process

As Figure 4-3 illustrates, information security risk management process can be iterative for risk assessment or risk treatment activities. An iterative approach to conduct risk evaluation can increase the depth and detail of the evaluation at each iteration. The

iterative approach provides the right balance between minimising the time and effort spent in identifying controls while still ensuring that high risks are appropriately assessed.

In an ISMS, establishing the context, risk assessment, developing the risk treatment plan and risk acceptance are all part of the “Plan” phase. In the “Do” phase of the ISMS, the actions and controls required to reduce the risk to an acceptable level are implemented according to the risk treatment plan. In the “Check” phase of the ISMS, managers will determine the need for revisions of the risk assessment and risk treatment in light of incidents and changes in circumstances. In the “Act” phase, any actions required including an additional application of the information security risk management process are performed. Table 4-1 summarises the alignment of ISMS and Information Security Risk Management Process.

ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Developing risk treatment plan Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process

Table 4-1 Alignment of ISMS and Information Security Risk Management Process

This research focuses on the “Plan” phase, which looks at different ways of planning for managing risks. In establishing the context, it will collect all relevant information about the organisation to identify the scope and boundaries of information security risk management to ensure that this information is considered in the risk assessment. Also, the gathered information should identify the organisational environment it operates in as well as how relevant it is to the information security risk management process.

During risk assessment in the information security risk management process, there are internal processes such as risk identification, risk analysis and risk evaluation. Risk identification will produce an output list of business processes to be risk-managed, a list of identified risk types and sources, a list of all existing and planned controls in their implementation and usage status and a list of incident scenarios with the consequences related to assets and business processes. Risk analysis will produce a list of assessed implications of an incident scenario concerning assets and impact criteria, the likelihood of incident scenarios (quantitative or qualitative) and a list of risks with the value levels assigned. Risk evaluation will produce a list of risks that are prioritised according to risk evaluation criteria regarding the incident scenarios that led to those risks.

Risk treatment options should be selected based on the outcome of the risk assessment, the expected cost of implementing these options and the expected benefits from these choices. Figure 4-4 shows ISMS' four options of risk treatment.

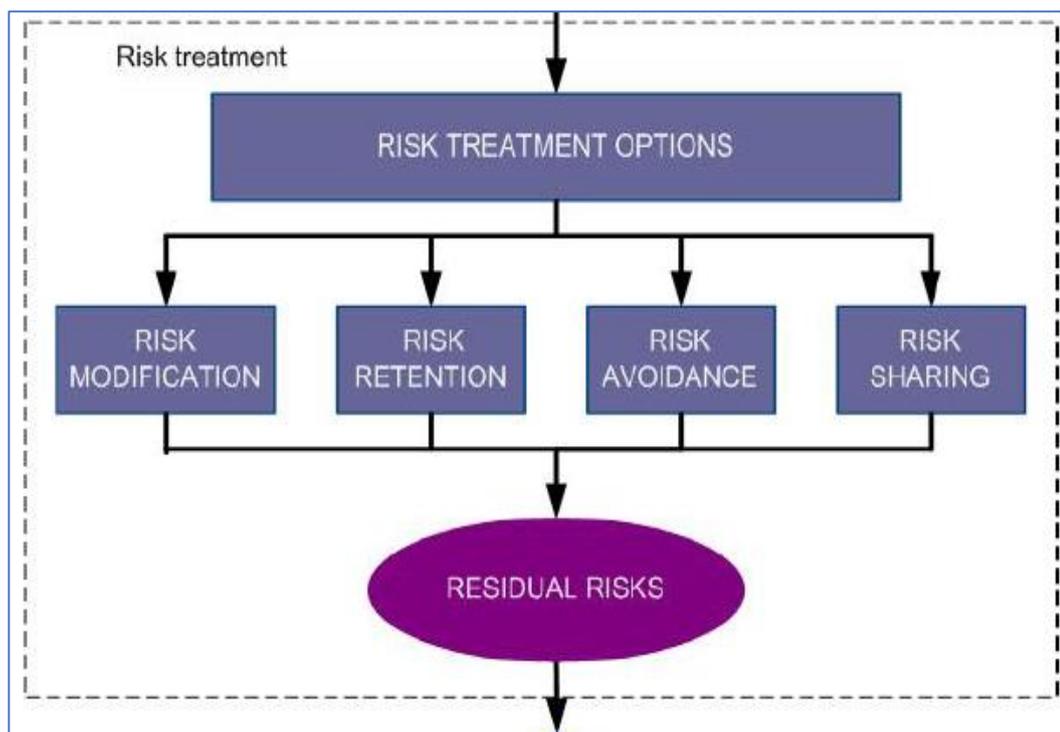


Figure 4-4 Risk Treatment Option

The four options of risk treatment are not equally exclusive. Sometimes the organisation can benefit significantly from a mixture of choices, such as reducing the likelihood of

risks, reducing their consequences, and sharing or retaining any remaining risks simultaneously. In practice, risk treatments can efficiently address more than one risk (e.g. information security training and awareness). A risk treatment plan should identify the priority order in which individual risk treatments should be applied and their timeframes (ISO 27005, 2011).

4.6 Analysis of the Different ISO Standards and Methodologies

There are many methodologies used to manage risk management. This section will provide an analysis of various standards; ISO 38500 for IT governance, organisational risk management methods based on ISO 31000 and an analysis of information security risk management methods based on ISO 27000 family of international standards. It will investigate the techniques these methods use to manage risks. A summary of each section is presented in a table which represents the name of the methods, how they are used, which ISO they are built on, advantages, limitations and which techniques they used to manage risks.

4.6.1 ISO 38500 IT Governance

Figure 4-5 presents the most common IT governance framework: Control Objectives for information and related technologies (COBIT) and how it aligns with other best practice frameworks, such as:

- Information Technology Infrastructure Library (ITIL), which is based (ISO 20000) on managing services in an organisation.
- PRINCE2/PRINCE2 Agile, which is used to manage new projects at high level.
- Project Management Body of Knowledge (PMBOK) is used as a reference for managing effectively.
- The Capability Maturity Model Integration (CMMI) is a process model that promotes behaviours that lead to improved performance.
- The Open Group Architecture Framework (TOGAF) aids designing, planning, implementing, and governing an enterprise's information technology architecture.

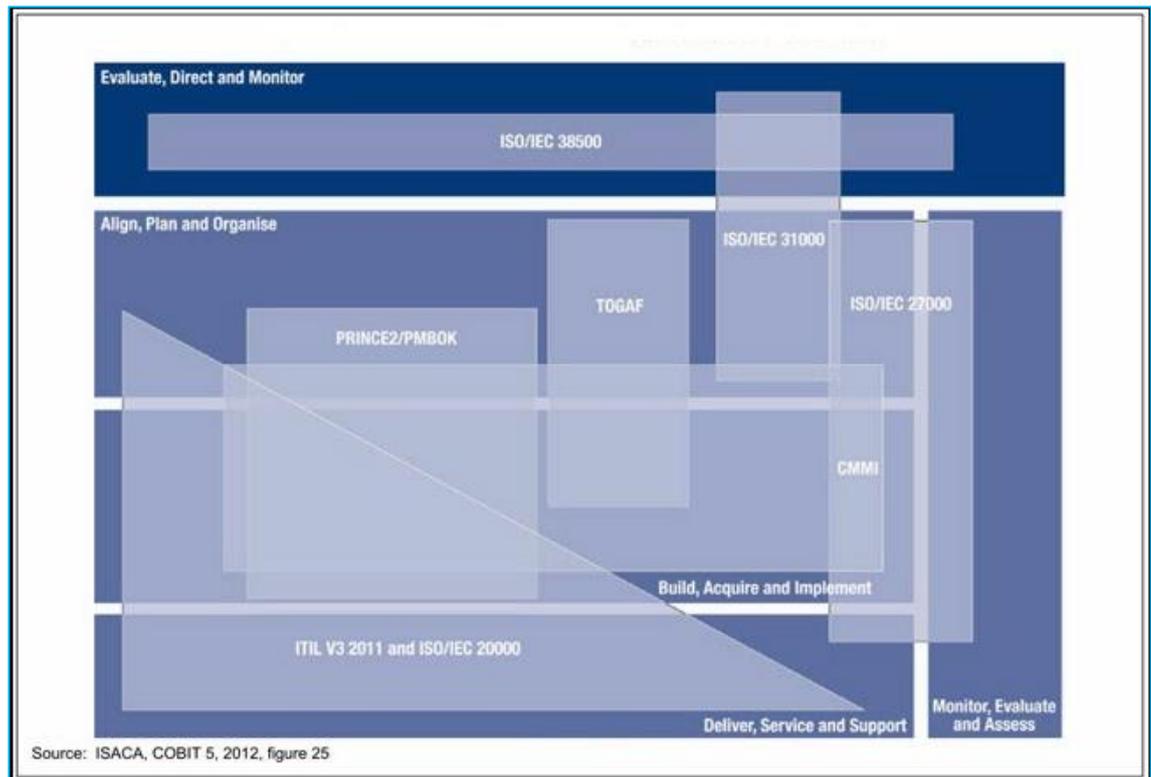


Figure 4-5 COBIT 5 For Risk of Other Standards and Framework
Source ISACA website, COBIT 5

COBIT 5 has several components that includes (ISACA, 2018):

- Framework, organises IT governance objectives and good practices of the IT domains and processes, and links them to business requirements.
- Process descriptions such as a reference process model and common language for everyone in an organization. The processes map shows responsibility areas related to planning, building, running and monitoring.
- Control objectives provide a complete set of high-level requirements to be considered by management for effective control of each IT process.
- Management guidelines help assign responsibility, agree on objectives, measure performance, and illustrate the interrelationship with other processes.
- Maturity models assess maturity and capability per process and help to address gaps.

Table 4-2 represents Governance framework method.

Name of Method	Type of risk it manage	What is it?	Use	Advantage	Limitations	Methods used for managing risks
COBIT	Governance framework	COBIT (Control Objectives for Information and Related Technologies) is a good-practice framework created by the International Professional Association ISACA for Information Technology (IT) Management and IT governance.	The purpose of COBIT is to provide management and business process owners with an information technology (IT) governance model that helps in delivering value from IT and understanding and managing the risks associated with IT. It uses ISO 38500	It has two processes which cover the governance domain and management domain	High level guidelines and risk management are embedded within its processes.	COBIT 5 for risk (domain APO12 Manage Risks) provides more extensive guidance and includes areas that are not covered by ISO 31000, such as IT risk governance and management. COBIT 5 for Risk addresses a comprehensive number of categories of IT risk, whereas ISO/IEC 27005 focuses specifically on information security risk. (Astuti et al., 2017)

Table 4-2 Governance Framework

4.6.2 Organisational Risk Management Methods

Some of the common methods in organisational risk management will be presented with a brief explanation. A comparison between Control Objectives for information and related technologies (COBIT) and Information technology Infrastructure Library, PRINCE2 and PRINCE2 Agile is presented. Then, a discussion regarding which technique each of these methods used to manage risks is provided.

COBIT and ITIL have been used by information technology professionals in IT Service Management (ITSM). When used together, COBIT and ITIL provide guidance for the governance and management of IT-related services in enterprises whether those services are provided in-house or obtained from third parties such as service providers or business partners (Năstase et al., 2009).

ITIL could be seen as the way to manage the IT services across their lifecycle while COBIT is concerned with how to govern the enterprise's IT in order to generate the maximum creation of value by the business, enabled by IT investments, while optimizing the risks and resources (Năstase et al., 2009). COBIT 5 describes the principles and enablers that support an enterprise in meeting stakeholders' needs, specifically those related to the use of IT assets and resources across the whole enterprise. ITIL describes in more detail those parts of the enterprise's IT that are service management enablers (such as process activities and organizational structures). COBIT is broader than ITIL in its scope of coverage (Năstase et al., 2009).

The distinction between the two is sometimes described as follows: "COBIT provides the 'why'; ITIL provides the 'how.'" (Năstase et al., 2009). It is more accurate to state that enterprises and IT professionals who need to address business needs in the ITSM area would be well served to consider using both COBIT and ITIL guidance (Năstase et al., 2009). Leveraging the strengths of both frameworks, and adapting them for their use as

appropriate will aid in solving business problems and supporting business goals achievement.

While ITIL improves existing services, PRINCE2® is used to develop projects that introduce new IT and services within organisations. PRINCE2® is a flexible method which guides one through the essentials of managing successful projects regardless of the type or scale used. It is built upon seven principles, themes and processes, and it can be tailored to meet specific requirements (Axleos, 2018).

In addition, PRINCE2 Agile® is not a replacement, but rather an extension of the PRINCE2® qualification. It has been designed to teach the fundamentals and purpose of combining PRINCE2® with Agile methodology. Combining them both provides scalability within corporate management processes (Axleos, 2018). Both PRINCE2 and Agile were developed as part of the technology industry to streamline the way projects are handled. However, PRINCE2 is gradually becoming a part of other industries whereas Agile's flexibility allows technical projects to evolve over time.

Management of Risks (M_o_R®) is a route map for risk management, which is bringing together principles, an approach, a set of interrelated processes, and pointers to more detailed sources of advice on risk management techniques and specialisms (Axelos, 2018). It also provides advice on how the principles, approach and processes should be embedded, reviewed and applied depending on the nature of the objectives at risk (Axelos, 2018). It also forms the framework for risk management in PRINCE2 and PRINCE2 Agile®. It is compliant with ISO 31000. In addition, it is embedded with ITIL and PRINCE2 depending on whether it is managing risks in services or within projects.

In terms of techniques used to manage risks, COBIT has developed COBIT 5 for Risk, which uses APO12 Manage Risks. [Figure 4-6](#) illustrates the scope of COBIT 5 for Risk. It shows that COBIT 5 for Risk focuses on applying the COBIT 5 enablers to risk through the risk function perspective (i.e., how to use COBIT 5). Also, it enables an effective and efficient risk governance and management function. It provides high-level guidance on

how to identify, analyse and respond to risk through the application of the core risk management processes in COBIT 5 and use of risk scenarios. The output is a document containing a list of IT risk assessment and risk control justifications which can be used as a reference document in managing risks associated with IT processes (Astuti et al., 2017).

Table 4-3 represents a summary of methods that address organisational risks.

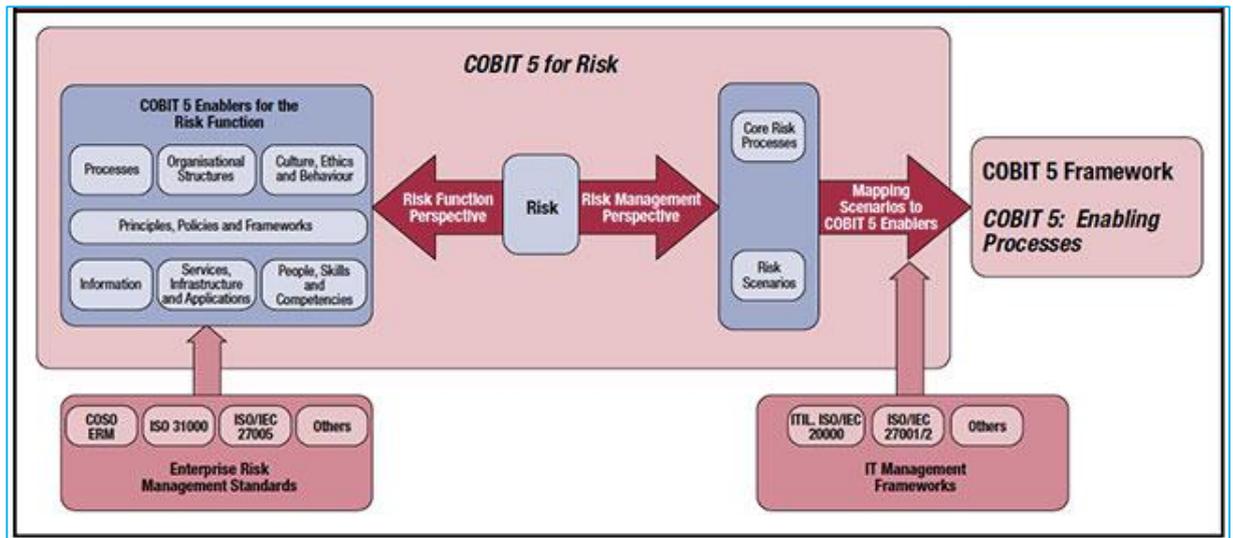


Figure 4-6 COBIT 5 for risk

Source: Information Systems Audit and Control Association (ISACA)

Name of Method	Type of risk it manages	What is it	Use	Advantage	Limitations	Methods used for managing risks
M_o_R Risk Management	Organisational risk	M_o_R is a route map for risk management. It can help organizations identify, assess and control risks and put in place effective frameworks for making informed decisions.	It also provides advice on how the principles, approach and processes should be embedded, reviewed and applied depending on the nature of the objectives at risk. It aligns with ISO 31000			It has four main process steps, which describe the inputs, outputs and activities involved in ensuring that risks are identified, assessed and controlled by using Risk register Source : (www.axelos.com).
ITIL	Service/Operational management	ITIL (Information Technology Infrastructure Library) is the most widely accepted approach to IT service management in the world. ITIL can help individuals and organizations use IT to realize business change, transformation and growth.	ITIL contains a comprehensive set of best practices for IT service management (ITSM) that are used to develop and execute IT service management to suit the needs of the business. It also aligns with ISO 20000. and has risk management within it	Manage business risk and service disruption or failure. Improve and develop positive relationships with your customers by delivering efficient services that meet their needs.	It is descriptive and not prescriptive so it needs internal processes in place to align with all its benefits. ITIL depends on how knowledgeable and willing the people that use it are. If they have a poor understanding of ITIL/ITSM, then the framework will not reach its maximum potential.	Mapping of M_o_R processes in ITIL sub-processes to manage risk Source : (Vilarinho and da Silva, 2011) ITIL Risk Management sub-processes called Business Impact and Risk Analysis uses risk register to prioritize lists of risks which must be subsequently addressed.

				<p>Establish cost-effective systems for managing demand for your services.</p> <p>Support business change whilst maintaining a stable service environment.</p>	<p>ITIL is weak in the risk management field.</p>	
PRINCE2	Project risk	<p>Providing guidance that gives individuals and organizations the essentials of running a project; PRINCE2 is easy to learn and a flexible method that can adapt to all types of projects.</p>	<p>It is a de facto process-based method for effective project management. Used extensively in the UK Government. PRINCE2 is also widely recognised and used in the private sector, both in the UK and internationally.</p> <p>It uses management of risk framework which aligns with ISO 31000</p>	<p>To increase quality of the finished products, efficient control of resources, avoidance of either "heroic" (under-regulated) or "mechanistic" (over-regulated) working, and increased confidence among the project team.</p>	<p>Considered inappropriate for small projects or where requirements are expected to change.</p>	<p>Use Risk Management procedure which uses Risk Register as a tool for capturing and maintaining information of identified risk.</p> <p>Source : (Tomanek, and Juricek, 2015)</p>

<p>PRINCE2 Agile</p>	<p>Project risk</p>	<p>PRINCE2 Agile® is the world’s most complete agile project management solution, combining the flexibility and responsiveness of Agile with the clearly-defined framework of PRINCE2®.</p>	<p>It provides structure, governance and controls when working with agile concepts, methods and techniques. Designed to help professionals tailor management controls when working in an agile environment; the new product will help the practitioner understand PRINCE2 governance requirements clearly and comprehensively as well as the interface between PRINCE2 and agile ways of working.</p> <p>It uses management of risk framework which aligns with ISO 31000</p>	<p>It allows for seamless integration with PRINCE2® and is therefore applicable to any type of projects. It makes use of common terminology across disciplines (meaning that the language used to deliver the course will be like that used in PRINCE2®).</p>	<p>Uses Risk Management procedure which uses Risk Register as a tool for capturing and maintaining information of identified risk .(Tomanek, and Juricek, 2015)</p>
-----------------------------	---------------------	---	---	---	---

Table 4-3 Organisational Risk

4.6.3 Methods of Managing Information Security Risk

There are numerous methods for managing information security risks and each method has its strengths and limitations. Some of the common methods for managing information security risks will be presented with a brief explanation. For this research, EBIOS, MEHARI, OCTAVE, MAGERIT, NIST SP800, CORAS were examined based on ISO 27000 family of International Standards.

EBIOS stands for Expression des Besoins et Identification des Objectifs de Sécurité - Expression of Needs and Identification of Security Objectives. EBIOS is a comprehensive set of guides dedicated to Information System risk managers. Originally developed by the French government, it is now supported by a club of experts of diverse origins (ENISA, 2018). It is a method for analysis, evaluation and action on risks related to information systems. It generates a security policy adapted to the needs of an organization and it has compliance with ISO 27001. EBIOS has a limitation, however, as the documentation available is in French. Therefore, it has not been widely adopted outside of French speaking countries (Gritzalis et al., 2018). In addition, it does not make use of scenarios, but rather follows a structured approach to identify and evaluate risk components. This offers the advantage of a relatively flexible and exhaustive risk analysis compared with other methods such as MEHARI, which are less flexible and use scenarios.

MEHARI is a method for risk analysis and risk management developed by CLUSIF (Club de la Sécurité de l'Information Français). It has compliance with ISO 27001 and ISO 27005 (Gritzalis et al., 2018). MEHARI aims to provide a set of tools specifically designed for security management, which comprises a set of managerial actions. It also provides guidelines related to security assessment (Syalim et al., 2009). The steps to conduct risk assessment include: Identifying risk, Evaluation of natural exposure, Evaluation of dissuasive and preventive factors, Evaluation of protective, palliative and recuperative factors, Evaluation of the potentiality of risk to occur, Evaluation of the consequences of the risk event actually happening, Evaluation of impact and impact reduction, Global risk evaluation to the organisation and Decision on whether the risk is acceptable. MEHARI provides supplementary documents for risk assessment (Syalim et

al., 2009). It also provides step-by-step guides which are lacking in other framework such as the NIST 800 and ISO 27000 series.

Another method, called MAGERIT, separates assets into nine categories and uses a scale with values from minimum to very high for the likelihood of realization of a threat. MAGERIT is a risk analysis and management methodology for information systems developed by CSAE (Consejo Superior de Administracion Electronica). It is compliant with ISO 27001 and ISO 27002. However, MAGERIT has a disadvantage as it does not make use of the concept of vulnerability (Gritzalis et al., 2018).

NIST800-30 is a risk management guide for information technology systems recommended by the National Institute of Standard and Technology (NIST). It has compliance with ISO 27001. It is a technical risk assessment. Organizational vulnerabilities and controls only come into play after the risks inherent in the IT infrastructure are addressed unlike the ISO 27005 where existing controls precede the vulnerability analysis. In NIST SP 800-30, risks to the IT infrastructure need to be identified from the ground up before incorporating mitigation afforded by the existing controls (Blank and Gallagher, 2012).

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) approach defines a risk-based strategic assessment and planning technique for security. The primary benefit of OCTAVE is related to connecting organizational objectives to information risk assessment and vulnerability management. For this reason, OCTAVE is developed as a flexible and self-modified approach to be customized for different organizations by their small IT teams and business (Amini and Jamil, 2018). This model can be integrated with other models and used as a hybrid model which would appear to be a significant opportunity for cloud computing. However, unfortunately, documenting all requirements and characteristics of this integrated approach, makes this model more complex for distributed and massive computing environments. The method for threat classification and identification is another disadvantage of the OCTAVE model (Amini and Jamil, 2018).

CORAS is a method for conducting security risk analysis. CORAS was developed under the Information Society Technologies (IST) program. One of the main objectives of

CORAS is to ‘develop a framework that exploits methods for risk analysis, semi-formal methods for object-oriented modeling, and computerized tools, for a precise, unambiguous, and efficient risk assessment of security critical systems’ (Vorster and Labuschagne, 2005). It has compliance with the ISO 27001 and ISO 31000 process (Gritzalis et al., 2018). However, the calculation and reasoning likelihoods in some cases may be complex and difficult due to the uncertainty of the risk analysis (Tran, 2017). In addition, it only supports modeling risks on-the-fly and there is a lack of features for translating the model into sentences and calculating and reasoning likelihoods (Tran, 2017). [Table 4-4](#) represents a summary of IT security system risks methods.

Name of Method	Type of risk it manages	What is it	Use	Advantage	Limitations	Methods used for managing risks
NIST SP800-30	IT Security System Risk	NIST SP 800-30 is a standard developed by the National Institute of Standards and Technology. Published as a special document formulated for information security risk assessment, it pertains especially to IT systems. It has been widely used for information security risk assessment globally, and is relevant to any business with an IT component.	To inform decision makers and support risk responses by identifying: (i) relevant threats to organizations or threats directed through organizations against other organizations; (ii) vulnerabilities, both internal and external, to organizations; (iii) impact (i.e., harm) on organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur. It has compliance with ISO 27001	It allows for mapping of vulnerabilities; it is-quantifiable in technical terms – according to the context of each security requirement.	NIST SP 800-30 is a technical risk assessment. Organizational vulnerabilities and controls only come into play after the risks inherent in the IT infrastructure are addressed.	NIST SP800-30 performs Risk management processes including: (i) framing risk; (ii) assessing risk; (iii) responding to risk; and (iv) monitoring risk. Also, it includes the risk assessment and the information and communications flows necessary to make the process work effectively.
EBIOS	IT Security System Risk	EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité - Expression of Needs and Identification of Security Objectives). EBIOS is a comprehensive set of guides dedicated to Information System risk	It is a method for analysis, evaluation and action on risks relating to information systems. It generates a security policy adapted to the needs of an organization. It has compliance with ISO 27001.	It follows a structured approach to identify and evaluate risk components. This gives it the advantage of a relatively flexible and exhaustive risk	EBIOS has a limitation as the documentation is available in French, therefore it has not been widely adopted outside of French speaking countries (Gritzalis et al., 2018). In addition, it does not	EBIOS has several steps, such as; identify risk, risk analysis, risk treatment, evaluation and study the context. The results can be recorded and summary documents will be produced (ENISA, 2018).

		managers. Originally developed by the French government, it is now supported by a club of experts of diverse origins (ENISA, 2018).		analysis, compared with other methods.	make use of scenarios.	
MEHARI	IT Security System Risk	MEHARI is a method for risk analysis and risk management developed by CLUSIF (Club de la Securite de l'Information Francais).	Risk analysis methods It has compliance with ISO 27001 and ISO 27005 (Gritzalis et al., 2018).			It has several steps: to identify risk, evaluation, and impact. Then it provides a risk assessment document (Syalim et al., 2009).
OCTAVE	IT Security System Risk	The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) approach defines a risk-based strategic assessment and planning technique for security.	OCTAVE approach has three phases; each phase is broken down into processes. Each process has certain activities that must be completed. Within each of these activities, different steps must be taken in order to achieve the desired outputs. The final result is that risk decisions can be based on the threat profile of different assets. Each threat profile contains information on which mitigation decisions can be based (Vorster and Labuschagne, 2005). It uses ISO 27000	The primary benefit of OCTAVE is connecting organizational objectives to information risk assessment and vulnerability management. For this reason, OCTAVE is developed as a flexible and self-modified approach to be	Documenting all requirements and characteristics of this integrated approach makes this model more complex for distributed and massive computing environments. The method of threat classification and identification is another disadvantage of OCTAVE model (Amini and Jamil, 2018).	OCTAVE has several phases to perform: Risk identification, Risk analysis, Risk evaluation, Risk assessment, Risk treatment, Risk acceptance, and Risk communication.

				customized for different organizations by their small IT teams and business.		
MAGERIT	IT Security System Risk	MAGERIT is related to risk assessment methods	<p>This separates assets into nine categories and uses a scale with values from minimum to very high for the likelihood of realization of a threat. MAGERIT is a risk analysis and management methodology for information systems developed by CSAE (Consejo Superior de Administracion Electronica).</p> <p>It is compliant with ISO 27001 and ISO 27002</p>		MAGERIT has a limitation as it does not make use of the concept of vulnerability (Gritzalis et al., 2018).	It manage risks through risk identification, risk, analysis, risk assessment, risk treatment and risk evaluation (ENISA, 2018).
CORAS	IT Security System Risk	CORAS is a method for conducting security risk analysis. CORAS is a model-based method for conducting security risk analysis. It provides a customized graphical language for threat and risk modelling.	CORAS was developed under the Information Society Technologies (IST) program. One of the main objectives of CORAS is to ‘develop a framework that exploits methods for risk analysis, semi-formal methods for object-oriented modeling, and computerized tools, for a precise, unambiguous, and efficient risk assessment of		The calculation and reasoning likelihoods in some cases may be complex and difficult due to uncertainty in risk analysis (Tran, 2017). It only supports modeling risks on-the-fly and there is a	The CORAS method provides a computerised tool designed to support documenting, maintaining and reporting analysis results through risk modelling.

			security critical systems' (Vorster and Labuschagne, 2005; Gritzalis et al., 2018). It has compliance with ISO 27001 and ISO 31000 process.		lack of features for translating the model to sentences and calculating and reasoning likelihoods.	
--	--	--	--	--	--	--

Table 4-4 IT Security System Risk

4.7 Managing Information Security Risk in Healthcare

Healthcare organisations consider patient information security among their top priorities. Modern healthcare is focused on providing the integrated Patient-Centred (PC) approach to provide holistic treatment care for the patient. This requires enabling PC flow of information within different healthcare providers. As a result, the Care Team (CT) can securely access the required information held in the system. Burnap et al. (2012) pointed out the importance of the information owner ensuring that information is not obtained by third parties for use beyond the agreed purpose of sharing information. They also stress that this information should not remain accessible to collaborators once the initial sharing is complete (Burnap et al., 2012) to avoid security risks. Securing patient information is part of the patient's safety initiatives that require healthcare providers to focus on prevention through better risk management. Yeandle et al. (2013) emphasised the importance of performing a risk assessment process and considering the resulting documentation within healthcare to help people understand their own risk better, develop a capacity to reflect in the moment and form links between current risks and their experiences and relationships, both past and present (Yeandle et al., 2013).

An organisation has to choose a typical risk classification system and select known names such as “risk domain”, “risk area”, or “risk categories”. Regardless of the terminology, the primary purpose is to identify risks across the full continuum of the organisation by categorising them into common types. Classifying risk into domains will help ensure that nothing is omitted. Common risk areas identified in healthcare include operations, hazards and financial, strategic, regulatory, technological and human capital risks. Traditional risk management has concentrated on categories of risk silos and how a particular risk might affect one aspect of organisational healthcare such as insurance costs. Although recognising such risks is a step in the right direction, stopping the analysis after a particular risk is identified may paint an incomplete picture (American Society for Healthcare Risk Management, 2011). Also, traditional risk management fails to take into account the effect of one risk upon another. Understating the relationship between risks allows for better employment of resources (people, money, time, ideas) and prevents repetition of effort. However, the impact of risk on one another has not been addressed. For instance, reducing the professional labour pool is likely to create a demanding and stressful work environment that, in turn, promotes weak areas in the

workplace. Different relationships between risks can be found in patient safety, consumer satisfaction, work-related injuries and productivity. Thus, the relationships between risks need to be recognised and analysed to support the core organisational goals such as providing safe and quality patient care.

According to the American Society for Healthcare Risk Management (2011), it is vital that organisations do not abandon the traditional risk management model, but rather expand upon this and refine it so that it may be applied to all risks. A more modern approach to the risk management model must employ a cross-disciplinary strategy to risk management (American Society for Healthcare Risk Management, 2011). The primary goal of risk management approaches is to highlight enormous risks to the entire enterprise whether those risks are regularly encountered within the hospital or other healthcare settings or they have never been considered. Once those risks are identified, the organisation is better able to determine an appropriate methodology to mitigate those risks.

Different risk management techniques commonly used in the healthcare industry are considered and discussed in detail in the next section.

4.7.1 Risk Register

Many organisations use a Risk Register to document the assessment of risk with appropriate countermeasures within an organisation. Risk Register is one of the essential tools in information security risk management. It is a valuable tool for documenting and prioritising, managing and treating identified risks facing an organisation. Patterson and Neailey (2002) defined risk register as *"primarily a tool which has enabled the risks within a project to be documented and maintained irrespective of geographical location, and has provided the platform for the reduction and mitigation plans to be developed for the high-level risks within the project"*. Also, there are various statements which describe the role of 'Risk Register'. Williams (1993) states that *'the risk register... has two primary roles. The first is that of a repository of a corpus of knowledge...The second purpose of the risk register is to initiate the analysis and plans that flow from it'*. Thus, risk register should be used to keep track of the different risks within projects (Williams, 1993). Also, Chapman and Ward (1997) pointed out that to allow for documentation of the sources of

the risk, their responses and classification, the risk register identification phase involves compiling a list, log or register (Chapman and Ward, 2003). Hence, they recognise that the documentation produced through the utilisation of Project Risk Management can be considered as a *'by-product...rather than a central concern'* (Chapman and Ward, 2003).

Moreover, Ward (1999) provided a more comprehensive vision by identifying that the purpose of the summary risk register is to help the project team review project risks on a regular basis throughout the project' (Ward, 1999). On the other hand, Barry (1995) uses the risk register as *'a comprehensive risk-assessment system'* (Barry, 1995). Thus, risk register is used as a formal method of identifying, categorising and quantifying the risks and providing the means for developing a cost-effective tool for controlling the risks. Carter et al. (1995) offer a very detailed version of a 'risk register', and they point out that *'the RISKMAN Methodology calls for a simple database of the risks in a project to be constructed from day one'* (Carter et al., 1995). In summary, having a complete risk register allows management to prioritise, manage or treat risks they are facing. Also, a risk register can ensure that everyone involved in the project understands the risks; hence, a mitigation plan is created for the most severe risks.

As an example of using risk register in healthcare, Desai et al. (2014) conducted a study to determine risk factors associated with perioperative mortality in patients undergoing Abdominal Aortic Aneurysm (AAA) repair nationally and used these risk factors to create a scoring system and a risk register to determine the mortality rate based on risk scores. The analysis used the National Inpatient Sample (NIS) from 2000 to 2010. A discriminant analysis was used to predict in-hospital mortality once the predictor variables were identified using a multivariate analysis. A risk register was created using established rates of rupture for various AAA sizes and estimating the average mortality for those patients. This risk was then compared with the in-hospital mortality risk using discriminant analysis to make recommendations on minimising the overall mortality rate as a function of aneurysm size and predictors of mortality. This study demonstrates that not all patients with AAA between 5 and 5.5 cm are candidates for surgery. Higher-risk patients may benefit from Endovascular Aneurysm Repair (EVAR), and those patients with smaller aneurysm sizes and few risk factors may benefit from observation. Women, patients with renal failure, and anticoagulated patients have a higher risk of the in-hospital mortality.

Patients who undergo EVAR have significantly lower in-hospital mortality rates especially those patients who have a ruptured AAA (Desai et al., 2014).

At Virginia Mason hospital in Seattle (U.S), a patient safety reporting system was used to provide reports of risk and harm from the front line of patient care. To quantify and prioritise safety opportunities, a risk register system was developed and implemented. The basic *risk register* concepts were refined to provide a systematic way to understand risks reported by staff. The risk register uses a comprehensive taxonomy of patient risk and algorithmically assigns each patient's safety report to 1 of 27 risk categories in three major domains (Evaluation, Treatment, and Critical Interactions). For each category, a composite score was calculated by event rate, harm, and cost. The composite scores were used to identify the "top five" risk categories, and patients' safety reports in these categories were analysed in greater depth to find recurrent patterns of risk and associated opportunities for improvement (Mansfield et al., 2015).

The top five categories of risk were easy to identify; they had distinctive "profiles" of rate, harm, and cost. The ability to categorise and rank risks across multiple dimensions produced insights that were previously not available. These results were shared with leadership; thus, served as an input for planning quality and safety initiatives. This approach provided actionable information for the strategic planning process while strengthening the Virginia Mason culture of safety (Mansfield et al., 2015). Therefore, the quantitative patient safety risk register serves as one solution to address the challenge of extracting valuable safety lessons from large numbers of incident reports and could profitably be adopted by other organisations (Mansfield et al., 2015).

As a practice of using risk register in the UK, The Trust Risk Register is used in London North West Healthcare for documenting risks. It is reviewed by the Executive Team, updated monthly and presented to the Integration Board to monitor risks post-merger and the Clinical Performance and Patient Experience Committee to provide assurance on patient safety and quality of services. The Risk Register status is formally reported to the Audit Committee and Trust Board and external bodies to provide assurance.

Kingston Hospital uses risk register to document different types of risks. Risks are escalated to the Corporate Risk Register (CRR) at a score of 8+. This has resulted in

identifying a large number of risks at a detailed level on the CRR (Kingston Hospital NHS Foundation Trust, 2017).

NHS Shetland uses risk register to enhance the staff knowledge of the types of risks that are likely to cause harm. Therefore, each department's log of all the risks recorded on the Datix system is referred to as a Risk Register. Each Manager/Head of Department is responsible for maintaining this register, ensuring the risk information it contains is up-to-date and that review dates have not expired. Heads of Departments must identify any high or very high-level risks believed impossible to manage at a departmental level or any risk that could adversely affect achievement of the Board's objectives or present a large loss to the organisation and bring these to the immediate attention of the relevant Director. Such risks will then be submitted by that Director to the Risk Management Group (RMG) to be considered for inclusion in the Corporate Risk Register. The RMG reviews the Corporate Risk Register every eight weeks, and regularly reports to the Board (Oxley, 2015)

Cardiff and Vale University Health Board (2017) use the Corporate Risk and Assurance Framework (the CRAF) which brings together the corporate risk register and assurance framework into one single document. It provides assurance on the delivery of the core purpose of "*Caring for People; Keeping People Well*" through robust risk management processes. A risk register is a documented and prioritised log of the overall assessment of a range of risks facing an organisation. The risks shown within the CRAF have been identified following an assessment of the principle risk of achieving or not achieving strategic objectives. The risks have been taken from a number of sources such as Clinical Board Risk Registers. By completing the risk register, the organisation can then work on how the risks they are facing can be prioritised or managed. The CRAF is updated on a bi-monthly basis to reflect the periodic review of Clinical Board and corporate risk registers. Regular exception reports are provided to the Board and the relevant Committee (Cardiff & Vale University Health Board, 2017).

4.7.2 Operationally Critical Threat and Vulnerability Evaluation (OCTAVE)

Operationally Critical Threat and Vulnerability Evaluation (OCTAVE) represents another alternative technique for managing risks in healthcare. According to Woody (2006) and Coleman (2004), three healthcare organisations of different scales and geographic locations decided to use OCTAVE as a risk assessment tool. A key component of OCTAVE is the interdisciplinary structure of the analysis team which enables healthcare organisations to create sound and efficient security policies (Woody, 2006; Coleman, 2004). OCTAVE methodology is well documented and is structured into three phases. OCTAVE phase one formulates information relating to the organisation and its business practices. Phase two is geared towards asset-based information security and technical vulnerability assessment. Phase three offers analysis of information gained during phases one and two, and forms a roadmap for long-term organisational protection strategies and mitigation plans to address midterm vulnerabilities relating to critical assets (Woody, 2006; Coleman, 2004).

Although the processes in each step are structured and well defined, there is enough elasticity to permit tailoring of the approach to meet the unique requirements of each organisation adequately. The differences and similarities observed during the three risk assessments strongly support the concept of a decentralised decision-making approach to information security in the healthcare industry. There were similarities found among organisations such as the merging of biomedical systems and network information systems, which exposed mutual threats and concerns that may be dominant throughout the industry regardless of the geographic location or size of the organisation. Applying a standard industry-recognised methodology to identify these risks offers due diligence to the process while allowing organisations to justify their choices by considering their unique conditions and differing capabilities to moderate these risks (Woody, 2006; Coleman, 2004). The same risk could be evaluated and prioritised differently by an organisation of a different scale. The limited resources of many organisations and the time needed to implement effective protection strategies has affected the decision that risks need to be mitigated, deferred or accepted. Thus, when prioritising risks for mitigation, the impact of the risks to the organisation should be considered (Woody, 2006; Coleman, 2004).

4.7.3 Failure Modes and Effect Analysis (FMEA)

Another commonly used risk management method implemented in healthcare is Failure Modes and Effect Analysis (FMEA) (Vincent and Honeck, 2004). According to DeRosier et al. (2002), the engineering community has used the Failure Mode and Effect Analysis (FMEA) technique as a proactive evaluation of vulnerabilities technique. FMEA focuses on processes that manufacture products and involves the calculation of a risk priority number through a three-variable equation where each variable is scored from one to ten. Medical device manufacturers use this process when evaluating their equipment (DeRosier et al., 2002). Chiarini (2012) used FMEA as a risk analysis tool to show an improved situation concerning the health and safety of nurses and physicians by calculating contamination as a risk of the activity and its causes inside the pharmacy department of an Italian hospital.

According to Quality-One (2015), FMEA is an assessment tool, but it does not eliminate risks. Although FMEA was useful as a risk analysis tool, it has many limitations including its bias toward severity ratings, its ever-increasing list of possible failure modes, and complexity of use as it is only as good as the members of the FMEA team using it (Quality-One, 2015).

To eliminate the weaknesses of FMEA, Health Failure Mode Effect Analysis (HFMEA) was proposed by the National Centre for Patient Safety (NCPS) with assistance from the Tenet Health System (Dallas). HFMEA is a 5-step process that uses an interdisciplinary team to evaluate a healthcare process proactively. The team uses process flow diagramming, a Hazard Scoring Matrix, and the HFMEA Decision Tree to identify and assess potential vulnerabilities. The HFMEA Worksheet is used to record the team's assessment, proposed actions, and outcome measures. HFMEA includes testing to ensure that the system functions efficiently and new vulnerabilities have not been introduced elsewhere in the system (DeRosier et al., 2002).

Li et al. (2017) investigated whether the healthcare failure mode and effect analysis (HFMEA) is a valid proactive method to apply to chemotherapy administration in the Chinese oncology inpatient setting. A multidisciplinary team created a flow diagram of the chemotherapy administration process. Possible failure modes were identified and

assessed using a hazard-scoring matrix. Using a decision tree, failure mode recommendations were made. Chemotherapy error rates before and after the HFMEA were compared. The results showed that five failure modes were identified with high hazard scores, and 15 recommendations were made. After the intervention, the chemotherapy error rate decreased significantly from 2.05% to 0.17%. Thus, the complexity of intravenous chemotherapy makes it vulnerable to error, and severe consequences. Multiple errors can occur during the ordering, preparing, compounding, dispensing, and administering of chemotherapy. The process of HFMEA helped reduce the chemotherapy error rate in Chinese hospitalised patients. The failure modes with the highest hazard score apparently resulted from the communication and organisation problems (Li et al., 2017).

Indeed, communication problems may often hide unclear or unshared responsibilities, roles, and procedures. One of the most significant challenges is the fear of negative consequences; nurses in China were found to be reluctant to report nursing errors. The low report rates of nursing errors may influence the results. Two critical factors arise here. First, it is likely that in underreporting results from fear of accusation, the nurses' satisfaction with the process is an indication that this transparent, collaborative, and consultative process reduces fear and encourages more honest responses. Second, the involvement of the interprofessional team underscores the shared nature of shared responsibility for errors and that errors are best detected early and reported to the team so they can act quickly, without individuals feeling fear of recrimination (Li et al., 2017).

4.8 Comparison of Risk Management Tools in Healthcare

Other risk management tools exist, such as Cause and Effect; these tools are called Ishikawa Diagrams and are also known as Fishbone. It is used to systematically list the different causes that can be attributed to a problem (or an effect). A cause-and-effect diagram can aid in identifying the reasons why a process goes out of control. However, the diagram, like other problem-solving techniques, is a heuristic (verifying) tool. In addition, the final diagram does not rank causes according to their importance and nor does it assess a particular aspect of the risk.

Another tool called Fault Tree Analysis (FTA) is a deductive (top-down) method of analysing system design and performance. It involves specifying a top event to analyse followed by identifying all of the associated elements of a system that could cause that top event to occur. FTA is an effective “lead-in” to robust experimental design techniques but it does not provide risk assessment.

Failure Modes and Effect Analysis (FMEA) have emerged as a powerful tool for avoiding costly product performance failures. Both product/design FMEA and process FMEA can help improve product reliability and reduce design and manufacturing costs. FMEA is a bottom up approach to failure mode analysis. It is an inductive process, which is performed after the detailed design phase of the project is complete. FMEA is a method to evaluate possible ways failures can occur in a design, process, system, or service. FMEA uses teams to improve the design, product, process, and/or service. However, again, it does not assess risk and it depends on the effectiveness of the team performing it.

The most common techniques for managing information security risk in healthcare were examined in this research. These are Risk Register (RR), Operationally Critical Threat and Vulnerability Evaluation (OCTAVE) and Failure Modes and Effect Analysis (FMEA). Risk Register is widely used to document risk assessment in the NHS in UK. In addition, three healthcare organisations have adopted OCTAVE as a risk assessment tool because it forms part of the interdisciplinary structure of an analysis team which enables health organisations to create efficient security policies. Failure Modes and Effect Analysis (FMEA) is widely used in healthcare as a risk management tool as discussed in section 4.6.3.

Therefore, Risk Register (RR), Operationally Critical Threat and Vulnerability Evaluation (OCTAVE) and Failure Modes and Effect Analysis (FMEA) were chosen to be examined based on the ISO 27005’s main stages. A comparison table was created to decide which tools are the most appropriate to use as shown in Table 4-5. Risk Register was the most appropriate method to consider because it is compatible with all the stages in the ISO 27005. Risk Register is widely used technique to manage risks as seen in its

adoption by a range of approaches such as COBIT, ITIL, PRINCE2 and PRINCE2 Agile. The next section will discuss Risk Register benefits and limitations in depth

ISO27005		OCTAVE	Risk Register	FMEA
Establish Context		Phase one: formulate information related to the organisation and its business practices.	Helps to report and communicate risks within an organisation.	FMEA works smoothly through the development phases of an investigation of past failures and creates preparatory documents, for instance, Failure Mode Avoidance past (FMA) failure.
Risk Assessment	Risk Identification	Phase two: asset-based information security and technical vulnerability assessment.	Identify risk name with a short description. Helps to identify risk type Security (S), Management (M), Technical (T) and Legal (L) by name.	Use risk priority number (RPN) to be calculated. The RPN is the multiplication of three factors: the “occurrence” (O), the “severity” (S) and the “detection” (D). RPN negatively changes team behaviour because teams select the lowest numbers to get below the threshold rather than the actual risk requiring mitigation.
	Risk Analysis		It identifies risks Level.	
	Risk Evaluation		It identifies Impact and Likelihood.	
Risk Treatment	Risk Modification	Phase three offers analysis of information gained during phases one and two and forms a roadmap for long-term organisational protection strategies and mitigation plans to address midterm vulnerabilities relating to critical assets.	It identifies the countermeasure in detail.	FMEA is an Assessment Tool, and it does not eliminate problems.
	Risk Retention (accepting)			
	Risk Avoidance			
	Risk Sharing			
Monitoring & Review		Gap	Countermeasure or action column will show any changes or modification in the risk.	Gap
Communication and Consultation		Gap	Countermeasure or action will show the communication with relevant parties to handle the risk.	Gap

Table 4-5 Comparison Between Managing Information Security Risk Techniques in Healthcare

4.9 Risk Register Benefits and Limitations

Risk register is an important component of the overall risk management framework. It is a tool that helps to track risks as they occur and can be created during the early stages of a project. From the analysis in section 4.7, it can be seen that Risk Register represents an essential element of different methods such as COBIT, MoR, ITIL, PRINCE2 and PRINCE2 Agile. A risk register is used to identify, assess, and manage risks down to acceptable levels through a review and update process.

The main benefit of risk register is that it records the details of all risks that have been identified, as well as provides an analysis of their severity and an action plan regarding how those risks can be treated to mitigate the risks. The risk register database can be viewed as a management tool for monitoring the risk management processes within the project. In addition, in Project Management Body of Knowledge project management, risk register is repeated in all the phases. For instance, risk register is created as an output from phase two to *identify risks*. In the third phase, *perform qualitative risk analysis*, risk register is updated as an output. In phase four, *perform quantitative risk analysis*, risk register is used as an input and is updated as an output. Similarly, for phase five, *plan risk response* and phase six, *monitor and control risks*, risk register is used as an input and update during the phases to be produced as an output. Thus, it represents an active living document during the whole project.

Furthermore, risk register represents the heart of our proposed methodology for managing information security risk which will be discussed in Chapter 5. However, there are limitations which need to be addressed. Having a large risk register to document risk assessment with appropriate countermeasures is not yet sufficient. It lacks visibility of the process and a shared understanding of risk associated with each role. Thus, it is necessary to enhance the risk register document through visualising the whole process especially when there is a complicated process that includes roles, processes, activities and multiple locations when different organisations are involved.

4.10 Information Security

Information security needs to be discussed in a wider context. Due to time limitation, it is not possible for this research to address all of the different perceptions of risks. As discussed in Chapter 3, this thesis will investigate security risks as the main concern identified from the preliminary interviews, questionnaires and undersecretary interview. Therefore, the scope of the remaining thesis will focus on developing risk assessment methodology that can clearly identify and represent information security risk.

Information security represents a valuable asset to any organisation that requires protection (Hong et al., 2003). Security combines systems, operations and internal controls to guarantee the integrity and confidentiality of information and operational processes within an organisation (Hong et al., 2003). Security is primarily achieved by controlling physical access to system components that are unique and use proprietary communication protocols (Awan et al., 2016). There is a wide range of information security definitions that are summarised in [Table 4-6](#).

Author/ Year	Information Security definition
Finne (2000)	The protection of information assets from accidental or intentional but unauthorised disclosure, modification, or destruction, or the inability to process that information.
Pipkin (2000)	The process of protecting the intellectual property of an organisation.
Goluch <i>et al.</i> (2008)	A risk management discipline, whose job is to manage the cost of information risk to the business.
Anderson (2003)	Emphasised a well-informed sense of assurance that information risks and controls are in balance.
Venter and Elo (2003)	The protection of information and minimising the risk of exposing information to unauthorised parties.

Table 4-6 Summary of Various Information Security Definitions

Within the context of this research, it is believed that these definitions are not expansive enough to address information security. It is more than an intellectual property (Pipkin, 2000), managing cost (Goluch et al., 2008) and unauthorised parties access (Venter and Elo, 2003). Although these authors identified essential aspects of

information security, their definitions are not broad enough as they are focusing on a particular problem rather than information security as a whole.

It is essential to consider information security not just as a technical issue, but also as a managerial issue. Kazemi et al. (2012) emphasised that information security is not only a technical matter, but a fundamental management issue; its primary purpose is to create a secure information environment. Whitman and Mattord (2012) supported this view by recognising that information security's purpose is to protect the confidentiality, integrity and availability of information assets whether in storage, processing, or transmission. This is achieved via the application of policy, education, training, awareness, and technology (Whitman and Mattord, 2012)

With the increased use of information technology by different parties such as IT specialists accessing information facilities, non-IT specialists conducting regular operations and members of the public as users using information technology through the internet, the threat of unauthorised users increases. Hence, one of the vital concerns is to have effective and efficient information security management within the organisation. Chahino and Marchant (2010) emphasised Information Security as a discipline governing the framework for the continuous cycle of safeguarding information and ensuring related regulatory compliance. In addition, Shostack (2012) pointed out that information security is the assurance and reality that information systems can operate as intended in a hostile environment.

Whitman and Mattord (2010) highlight that information security, in general, can only be implemented through a process of institutionalisation (Alshaikh, 2014). They propose a security system development lifecycle (SecSDLC) consisting of six phases (Investigation, Analysis, Logical Design, Physical Design, Implementation, and Maintenance and Change) designed to implement an information security project in an organisation. These phases allow collaboration among IT managers, business units, and information security experts to rigorously design, develop, implement, and operate an information security program. Unlike traditional system development life cycles that employ the waterfall approach, the SecSDLC is an iterative process which enables agile and flexible changes during the design, development, and

implementation of the security program (Alruwaili and Gulliver, 2015). However, one of the disadvantages of SecSDLC is that it is interpreted as a waterfall model. The waterfall model does not allow changes to be made to the previously completed stage. Therefore, it would be implemented with missing/faulty requirements or mistakes committed at any stage of system development. Fixing such mistakes is not easy; it is costly and leads to late delivery of the requested system (Sekgweleo, 2018).

However, SecSDLC is an iterative approach which is similar to a spiral model. The emphasis of the spiral model is to evaluate risks, which are used as a source for decision making to further develop the system. This approach makes it possible for organisations to save costs since it is cheaper to identify problems and risks in the early stages of the systems' development. It also makes it possible to enhance or make changes to the requirements up until the acceptable system is delivered to the users (Sekgweleo, 2018).

Therefore, there is a trade-off between the flexibility and security approach lifecycle. In a complex system, it is hard to address all security issues within it whilst maintaining flexibility. Prior to initiating an information security program, it is advised that organizations have clear security policies and compliance requirements (Alruwaili and Gulliver, 2015). It is the company's responsibility to choose a suitable approach which can be tailored according to its need.

In this research, it is believed that using the risk management standards as they are does not provide enough guidance; therefore, it is important to have a shared understanding of the processes within the context where security is being applied. The role of process modelling prospected in risk management framework will be considered. The next section will provide an overview of Business Process Modelling (BPM) which has been used to model information security in healthcare processes.

4.11 Business Process Modelling (BPM)

Business Processes Modeling (BPM) represents an important part of an organisation because having an effective business processes is vital in sustaining competitiveness (De Sousa, 2014). It plays an essential role in two ways. The first functions at the operational management level: conducting and improving how the business is operated. Second, BPM is essential for software developers as they need a business process to capture the necessary requirements for software creation and design. BPM can reduce the distance between the users of the systems and its developers (De Sousa, 2014).

At the business process level, customers, end users, and business analysts can express their security needs. Rodríguez et al. (2007) proposed integrating security requirements through business process modelling through BPMN. In addition, Secure*BPMN was introduced (Cherdantseva, 2014) to cover security requirements in BPM. Thus, Business Processes can be defined as a set of procedures or activities that collectively keep track of a business objective or policy. Also, it represents a feasible solution to address the environment's complexity and the speed required for new products as well as the growing number of involved actors in the activities of the organisation (Rodríguez et al., 2007).

An enhanced definition of Business Process Modelling (BPM) is, *“a collection of activities that takes one or more kinds of input and creates an output that is of value to the customer”* (Stavrou et al., 2014; Gritzalis et al., 2014). It consists of a set of activities and tasks that, together, fulfil an organisational goal. By modelling activities and functions processes within an organisation, it can provide a holistic approach and improve the understanding of goals within the workplace. BPM can reduce costs and offer competitive products and services (Stavrou et al., 2014). Furthermore, BPM has increasingly been recognised as a driver for innovation (Rosemann, and Brocke, 2015). According to Aagedal et al. (2002), using BPM to model risk assessment is motivated by several factors; risk assessment requires correct descriptions of the target system, its context and all security features. The modelling technology improves the precision of such description; the latter is expected to improve the quality of risk

assessment results (Aagedal et al., 2002). In addition, the graphical style of BPM furthers communication and interaction between the stakeholders involved in a risk assessment. This is expected to improve the quality of results, and also accelerate the risk analysis process since the danger of wasting time and resources on misconceptions is reduced (Aagedal et al., 2002). Modelling technology facilitates a more precise documentation of risk assessment results and assumptions on which their validity depend. This is expected to reduce maintenance costs by increasing the possibilities for reuse (Aagedal et al., 2002). Modelling technology also provides a solid basis for the integration of assessment methods that should improve the effectiveness of the assessment process (Aagedal et al., 2002). Aagedal et al. (2002) point out that modelling technology is supported by a rich set of tools from which the risk analysis may benefit, such as improving quality and reducing costs. It also increases productivity and facilitates maintenance. This provides a basis for tighter integration of risk management in the system development process, which may considerably reduce development costs and ensure that the specified security level is achieved (Aagedal et al, 2002). Therefore, the Aagedal et al. (2002) findings represent a solid basis for using modelling in managing risks.

4.12 Examples of Using BPM to Model Security

Rodríguez et al. (2007) proposed integrating security requirements through business process modelling. They emphasised the importance of capturing security requirements within business process modelling through notations that must be supported by a set of graphical concepts that allow for the security semantics to be represented (Rodríguez et al., 2007). BPMN offers orientation to the business analyst domain since it represents an opportunity to capture security requirements at a level of abstraction. They presented the BPMN meta model with core elements and extensions that allow security requirements to be incorporated into Business Process Diagrams that will increase the scope of the expressive ability of business analysts. With this extension, business analysts will be able to express security requirements from their perspective. Moreover, it will be possible for security experts to refine such requirements for software developers to be able to include them in the end product. They applied this approach within a typical health-care business process (Rodríguez

et al., 2007). However, this approach has limited expressiveness as it does not take into account the information flow of business processes, and it does not decouple the specification of the policy from the modelling of the security solutions that the process implements.

Saleem et al. (2012) extend BPMN with security objectives for Service-Oriented Architecture (SoA) applications. They include a set of security concepts in BPMN such as confidentiality, integrity, availability, traceability, and auditing. However, the language does not separate policies from security solutions in the processes. Moreover, their work is specific for the SoA domain (Salnitri et al., 2017)

Wolter et al. (2009) propose a modelling language for business processes and business security goals that should be used to graphically define security specifications. They also developed a framework which transforms security goals in security policies specified in XACML and Rampart (Salnitri et al., 2017). The framework automatically extracts specifications of security mechanisms which enforce the security goals, but it does not permit security experts to compose security goals; therefore, it does not permit the creation of complex security policies (Salnitri et al., 2017).

Wolter and Schaad (2007) propose an extension of BPMN for specifying task-based authorization constraints. Their approach includes a graphical extension of BPMN as well as a formalization of task-based authorization constraints. Their approach permits the specification of dynamic resource allocation such as dynamic separation of duty and role-based resource allocation. Their approach is focused on authorization constraints on executors of tasks. In addition, it is not possible to use this approach to specify other security aspects such as availability or integrity (Salnitri et al., 2017).

SecureBPMN (2012) extends BPMN with access control and information flow constraints. It uses the hierarchical structure of the organization in which the business process will be executed to help security designers to define security properties such as the binding of duty and separation of duty. However, SecureBPMN is limited in that it does not specify other central security aspects, such as confidentiality or availability (Salnitri et al., 2017).

Alsalamah (2014) looked at the security requirements of the patient-centric by using workflow. She focused on providing different security levels while the information is shared across healthcare organisations holistically. She modelled the access control permission. On the other hand, this research will focus on risk modelling and enhance the communication mechanism among stakeholders.

Cherdantseva (2014) developed Secure*BPMN. The semantics of Secure*BPMN were based on the Reference Model of Information Assurance and Security (RMIAS). RMIAS is based on the ISO 27001 and is intended for communicating Information Assurance and Security (IAS) concepts to business experts and other non-technical audiences. It reflects a shared understanding of IAS and it is suitable for an approach to IAS in a multidisciplinary team. The syntax of Secure*BPMN was designed specifically for human understanding and communication improvement purposes (Cherdantseva, 2014). Also, Secure*BPMN added additional security classes like Secure Swimlane, Secure Swimlane location, Access Permission, Information Taxonomy, Security Goals and Countermeasures.

Conforti (2014) developed an operational approach for the management of risks related to executable business processes in near real-time. It incorporates elements of risk in all stages of the lifecycle of executable business processes. His work contributes to creating a more effective link between the fields of Business Process Management and Risk Management. He developed a working BPM system with risks expressed formally and managed dynamically in the workflow. The approach was implemented over the YAWL system and evaluated through the use of artificial and real-life data. (Conforti, 2014).

Jakoubi et al., (2010) presented a methodology enabling the risk-aware modeling and simulation of business processes. The term 'risk-aware business process management' is understood as the integration of a risk perspective into business process management. In addition, their work provides a readable overview of academic research on integrating risk management into BPM (Jakoubi et al., 2010).

Koster (2009) proposed an evaluation method for Business Process Management products. This method was developed by creating a framework on BPM by analysing the state of the literature regarding BPM. This framework contains literature and criteria that have been extracted by the literature in the field.

Although other researchers used risk modeling in an algorithmic way using quantitative approaches to risk, our approach is qualitative and focuses on representing risk within Business Process Modelling. It ensures that it is linked with risk register to document the risk assessment. This research will address the application of Managing Security Risk-Business Process Modelling in the next chapter.

4.13 Reflection

There has been an extensive range of standards and normative documents presenting risk management and risk assessment methodologies for IT systems over recent years. Studying the ISO 38500 for the IT governance framework was important as it helps in understanding business requirements. The ISO 38500 for the IT governance framework helps to ensure that accountability is clearly assigned for all IT risks and activities. It encompasses assigning and monitoring IT security responsibilities, strategies and behaviours.

In addition, it is important to understand the different methodologies based on the ISO 31000 for organisational risks to be aware of the different methods available for managing system risks. Also, the ISO 27000 family of standards was addressed to observe the different methods used in managing information security risks.

It is not easy for the practitioners to know what technique to use because there is a wide range of standards that hold different methods and techniques, which can be applied at different levels depending on the scope of an organisation. Thus, a comparison section for different ISO standard methods was needed to understand how each method works, how it is used, which standard has compliance, advantages, limitations and what technique are used by each method to manage risk. The

effectiveness of these standards and methods in supporting practitioners of risk management will depend on the organisation and how often these standard techniques are carried out. For instance, the ISO 31000 is used for organisational risk and ISO 27000 is used for information security risk.

There are limitations in the use and application of different tools and techniques in managing risks. For instance, ISO 27000 requires continuous subjective input by the stakeholders to calculate potential risks. Hence, it requires subjective, human-based qualitative inputs, which could potentially lead to inaccurate and inconclusive results (Awan et al., 2016). Also, the main research challenges relate to the application of the ISO 27000, which is a high-level guideline in the healthcare domain. It does not provide detailed step-by-step guidance or advise on which technique to use. Operational Critical Threat and Vulnerability Evaluation (OCTAVE) was used in Risk Management (ISO 31000) and in the healthcare domain to minimise the identified risks. However, it is not practical for the entire process within the ISO 27005 because it does not cover all the stages for monitoring and review, and communication and consultation.

Failure Modes and Effect Analysis (FMEA) is more of an analysis tool for risks. It does not address how to manage the identified risks. The risk register can be used in all the stages of the ISO 27005 processes within the healthcare industry to document and prioritise risks, but its limitation is that it does not visualise the risks in a process. Therefore, it is necessary to develop an effective approach which can address risk and enhance communication among stakeholders and locations.

4.14 Conclusion

Information security risk management represents a critical element within any organisation; hence, it requires deep understanding and awareness in terms of what the best approach is according to the organisation's aims and objectives. Therefore, studying IT governance framework (ISO 38500), Risk Management (ISO 31000), Managing Information Security Standard (ISO 27000) and Information Security Risk Management Standard (ISO 27005) helped in understanding and identifying various types of risk management methods and techniques that are implemented in multiple industries.

As the focus of this research is the healthcare industry, common tools used to manage risks were observed and critically analysed. Those tools were: Risk Register (RR), Operational Critical Threat and Vulnerability Evaluation (OCTAVE) and Failure Modes and Effect Analysis (FMEA). A comparison table based on ISO 27005 was created to understand which method was applicable for the research domain. From the comparison table, Risk Register was considered as the most appropriate tool to use because it was compatible with all the ISO 27005 processes. However, there are limitations in the use of Risk Register to document the risk assessment as it does not visualise the risks at process level.

Business Process Modelling (BPM) was considered as a tool for understanding risks and enhancing communication within different locations. This chapter discussed various examples related to using BPM in healthcare. Although other researchers addressed security requirements and meta model (Rodríguez et al., 2007) and risk modelling through algorithmic approach (Jakoubi et al., 2010), this research proposes a different approach to using risk register to document risk assessment and represent risks in a business process modelling by visualising risks within a process and providing a shared understanding of risks for stakeholders.

In Chapter 5, Managing Security Risk-Business Process Modelling (MSR-BPM) will be introduced as an effective approach to manage risks by combining Risk Register and Business Process Modelling (BPM). In Chapter 6, MSR-BPM approach will be applied in the healthcare domain to identify risk assessments and security goals in depth.

5 Chapter 5: Methodology Framework

5.1 Introduction

This chapter proposes an approach to effectively manage risks by addressing visibility and shared awareness of risk. It introduces using a Reference Model of Information Assurance and Security (RMIAS) (Cherdantseva, 2014) to develop Generic Reference Risk Register Table. The methods analysis in Chapter 4, section 4.7 shows that the risk register represents an essential element of many methods. These methods tended to adopt various techniques to produce the risk register document to help decision makers within an organisation. However, there are limitations in using the Risk Register alone as it lacks risk visibility within a process.

The Methodology was enhanced to explicitly represent risk. Secure*BPMN (Cherdantseva, 2014) was expanded by adding risk representation to it. The main processes in Information Security Risk Management (ISO 27005) were used as a basis to combine Risk Register and Business Process Modelling as an approach to manage security risks. This chapter will also explain the procedure taken to create Managing Security Risk – Business Process Modelling (MSR-BPM) as an approach to manage risks.

The central purpose of using MSR-BPM is to help organisations prioritise, manage and provide options for treating the identified risks as well as provide a shared understanding of risks according to the stakeholder role, whether it is a process or activity risk. In addition, the approach provides traceability of risks to monitor risk modification and location. The use of MSR-BPM is reflected upon to explore the challenges that might occur during the implementation process as well as identify its limitations and potential usage in different industries.

5.2 Using RMIAS to Develop a Generic Reference Risk Register Table

As discussed in Chapter 4, Information Security Management Systems (ISO 27001) is the most widely used security risk management standard; it is implemented in 163 countries. ISO 27001 provides high-level guidelines for managing security risk, but it is complex and lacks detailed guidance. Using the ISO 27001 standard source document alone is, therefore, not sufficient to implement effective information security management systems (ISMS) for organisations. Detailed guidelines are required as various processes and controls are merely described in the standard without detailing the "how to" implement for practitioners. Providing detailed guidance for standards surfaced as a need to facilitate better understanding and to encourage wider adoption (Al-Ahmad and Mohammad, 2012).

Therefore, an effective methodology is necessary to manage security risks holistically. Thus, research on the available literature was conducted to identify a framework; ISO 27001 was adopted as a basis to expand the method. Reference Model of Information Assurance & Security (RMIAS) (Cherdantseva, 2014) is based on Information Security and Information Assurance standards and ISO/IEC 27000 family of standards; hence; RMIAS was adopted as part of the methodology framework. The RMIAS is the culmination of the analysis of the Information Assurance and Security (IAS) literature. It is a synthesis of the existing knowledge of the Information Assurance and Security (IAS) domain. It is intended for communicating IAS concepts to business experts and other non-technical audiences. It works at the level of high abstraction ignoring issues such as technical, legal or other issues, with which a non-technical, non-security and business audience may be unfamiliar (Cherdantseva, 2014).

Also, the RMIAS is generic as any reference model should be. It tries to cover the aspects of IAS, which are relevant to the majority of organisations. This indicates that the RMIAS requires adaptation when being applied in the context of a particular

organisation. The RMIAS is flexible and allows organisation-specific adjustments (Cherdantseva, 2014). Hence, it can be adapted to the healthcare industry. Furthermore, the structure of the RMIAS is flexible to permit extensions, which may be necessary due to changes in an environment, society and technology. The current dimensions may be extended; for instance, new security goals, new types of security countermeasures may be added to the RMIAS or the information taxonomy may be extended and even new dimensions may be introduced (Cherdantseva, 2014).

Figure 5-1 depicts RMIAS framework, which has four dimensions:

- Security Development Life Cycle Dimension (top left quadrant) demonstrates the progression of IAS along the Information System Development Life Cycle (ISDLC),
- Information Taxonomy Dimension (top right quadrant) shows the characteristics of the 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 classifies security countermeasures.

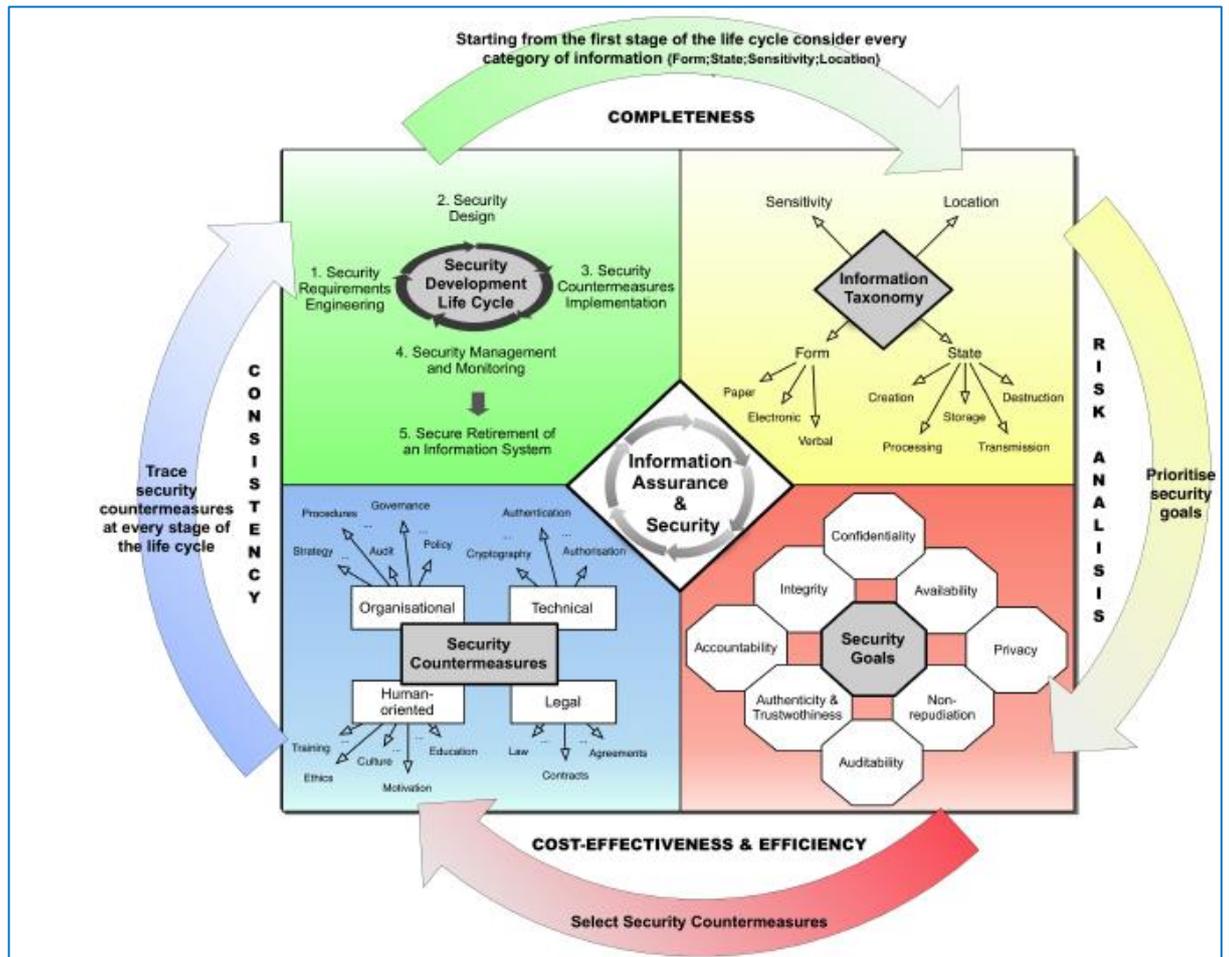


Figure 5-1 The Reference Model of Information Assurance & Security (RMIAS)

The RMIAS, starting from the top right quadrant, point out (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 attained (the security countermeasures dimension) and (4) the cycle of security activities ensuring that the concepts of the other three dimensions are sufficiently addressed at every stage of the life cycle (the security development lifecycle dimension) (Cherdantseva, 2014).

The four dimensions of the RMIAS do not overlap and do not duplicate each other. RMIAS starts from the top left quadrant. An organisation defines its current stage of the security life cycle and then goes over the other three dimensions to come back to the next stage of the life cycle. At the stage of requirements engineering, an organisation inventories its information assets, establishes and prioritises security

goals and selects security measures. At the stage of security design, an organisation ensures that all information assets, goals and measures identified in the previous step are consistently incorporated into and addressed by the system models. At the stages of implementation and management/monitoring, it must be ensured that (1) all countermeasures are implemented and function as designed and (2) the established security goals are achieved for every category of information (Cherdantseva and Hilton, 2014).

The discussion provided by Cherdantseva and Hilton (2014) can be interpreted as a waterfall method. An organisation will move through four quadrants of the security system development lifecycle once. However, we need to be aware that the security system can be delivered in an iterative way and, in that case, an organisation will go through each of these four quadrants in each iteration rather than going through each phase of the life cycle in a sequential way.

According to Salnitri et al., (2014), RMIAS is the result of an analysis and classification of security aspects proposed by a reference model on information assurance and security because it provides the most comprehensive set of security aspects. In addition, the RMIAS is used to help the organisation to revise the Information Security Policy Document (ISPD) to reflect the new circumstances because it undertook major changes to its business (Cherdantseva and Hilton, 2014).

Although RMIAS provides a comprehensive view of information security, it did not cover risk management in detail. Risk analysis is marked in RMIAS underneath the yellow arrow on the right-hand side (see [Figure 5-1](#)) to prioritise security goals. According to Cherdantseva and Hilton (2014) “*The RMIAS is not Risk Analysis (RA) methodology, but it points out an important place of RA in the IAS domain and articulates the requirements towards an RA methodology which should assist with the creation of a detailed inventory of information and facilitate the prioritisation of security goals*”. Risk analysis is a critical area in any domain; therefore, it needs to be addressed carefully and holistically. RMIAS did not address risk management in detail nor produce risk register as an output. The proposed approach in this research will address this gap.

RMIAS was used as a basis to structure the proposed process. Security Development Life Cycle Dimension (the top left quadrant) was replaced with the Information Security Management System (ISMS) processes in [Figure 5-2](#) . It is believed that a risk management process is more appropriate because we are looking at risks that relate to a particular scenario or operational process rather than looking at the whole security system development life cycle.

The proposed approach will use risk management process from ISO 27005 because it is an appropriate methodology for our domain to improve the ongoing process at the operational level to provide a shared awareness of security risk.

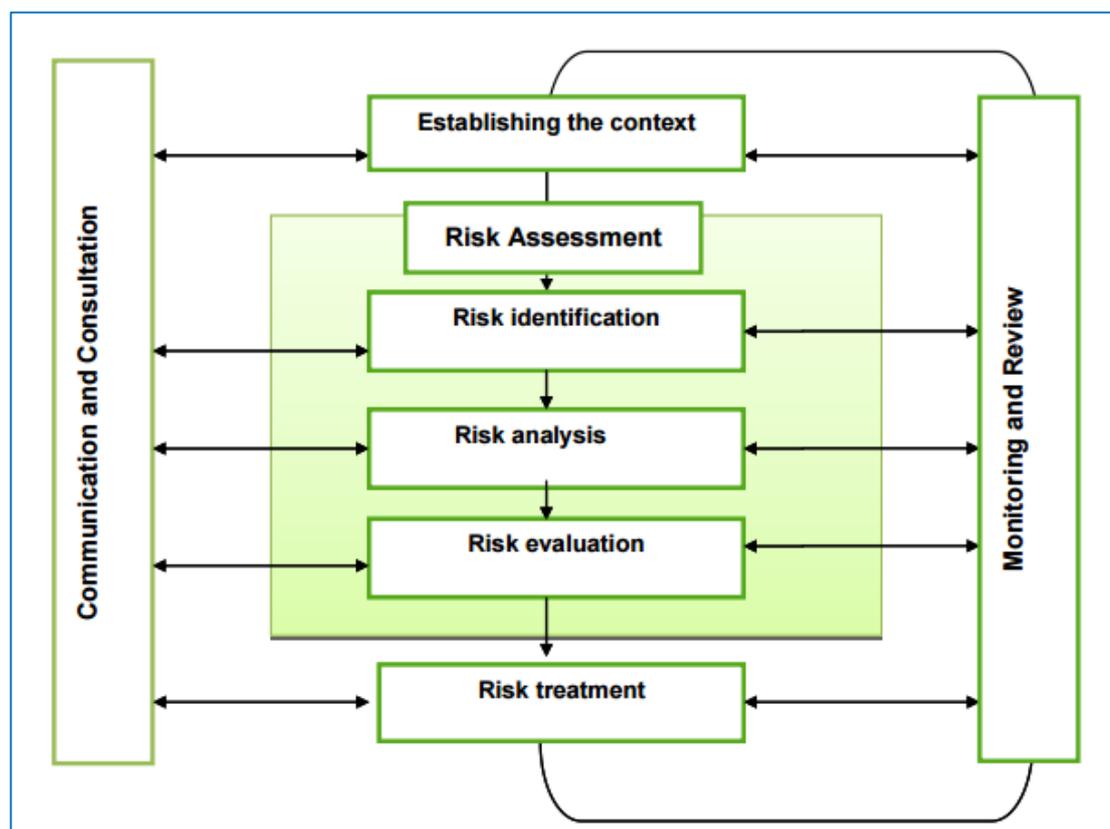


Figure 5-2 Information Security Risk Management ISMS Processes

RMIAS was used to develop a generic risk register table to document the risk name and risk description. The structure of the risk register was used to determine the taxonomy of risk information such as risk identification, risk analysis and risk evaluation.

The European Union Agency for Network and Information Security (ENISA) was used as a trusted source to identify the impact, likelihood and risk level for each risk because the researcher did not have the domain knowledge for risk evaluation. Table 5-1 provides a sample of risk evaluation. This is an important analysis as it will show the decision makers which risk is critical and requires immediate mitigation and which risk is not significant to be managed. Other risks can be shared or transferred to another party.

No	Risk Type	Risk Name/Description	Impact	Likelihood	Risk Level
1	Security	Safeguarding patient confidential information and compliance .	Very High	Medium	High
		<i>Description</i> Guaranteeing security in storing medical health records and safeguarding it with key regulations.			

Table 5-1 Sample of Risk Evaluation to Risk Register

As RMIAS was applied to structure our thinking in creating the risk register, it was also used to identify security goals applicable to each risk because it addresses all the security goals in ISO 27000. Thus, a new column for security goals will be added to the risk register table. Having security goals within the risk register table may help in determining the countermeasure needed to modify the identified risk.

Afterwards, a new column for security countermeasures was added to identify the adequate countermeasure for each risk. In some risks, more than one countermeasure is needed, for instance, technical and organisational. The details of each countermeasure will be discussed further in Chapter 6 when applying the hypothetical scenario. At this point, it can be clearly seen that RMIAS was used as a basis for creating a risk register table that lists the risk name, risk evaluation, security goals and security countermeasure.

Since the healthcare industry is focus of this research, Health Informatics-Information security management in health (ISO 27799:2008) and Health Informatics-Information security management in health (ISO 27799:2016) were utilised for identifying appropriate countermeasures such as information security document and access control policy.

Forty-six risks of different types were identified through the literature published by the European Union Agency for Network Information Security (ENISA, 2012), Latif et al. (2014) and Mxoli et al. (2014). These risks could be categorised as Security, Management, Technical and Legal risks. Each risk's name is briefly described, and customised according to the situation. In addition, each risk is critically evaluated according to healthcare context in the Government of Oman by using one of the two Omani cloud computing providers: Oman Data Park (ODP) or Information Technology Authority - Cloud (ITA-Cloud). ODP and ITA-Cloud hold the ISO 20000 (IT service management) and ISO 27001 (Information Security Management System) certifications. These certifications confirm that ODP and ITA-cloud have an advanced IT service management that matches a globally recognised standard. In addition, they have Tier 3 certified "TIA 942 rating" and 24/7 Security Operations Center (ODP, 2019).

As discussed in Chapter 2, Ministry of Health (MoH) in Oman uses cloud computing infrastructure to host the ministry's website. It does not provide electronic health records to the patient. However, Cloud computing can provide the necessary future infrastructure for electronic health records because of its flexibility and accessibility. It can be utilized as a central repository for hospitals as it is capable of providing hospitals with the necessary on demand services, better authentication/authorization and data backups. In addition, it will allow scalable and elasticity demand for e-Health services. Healthcare professionals will be able to attend to their patients from anywhere at any time. Despite the wide range of benefits for using cloud computing services, there are risks relating to the project set up. Examples of these risks include Change Project Risks that arrive from migrating to the cloud, Operational Level Risks associated with the cloud Infrastructure managed by ODP and ITA-Cloud and

Operational Level Risks that will be managed by hospitals. The three types of risks will be discussed in general at this stage and they will be included in the generic reference risk register table which can be found in [Appendix C](#).

Although the initially discussed risks from the literature represented different types of risks, such as Management, Legal, Technical, and Security risks, the mapping process of survey questions in Chapter 3 ([Appendix B](#)) identified various risks such as Internet-based services, Human, Privacy, Technology, Organisational and Environmental risks in detail. Thus, an extra column was added for the perceived risks. This process showed that many survey questions were found in the literature (Mxoli et al., 2014; Latif et al., 2014) and this represented a major concern regarding risks. [Table 5-2](#) represents a sample row of the updated risk register table.

No.	Risk Type	Risk Name/Description	Impact	Likelihood	Risk Level	Risk Perception	Security Goal	Security Countermeasure
1	Security	Safeguarding patient confidential information and compliance.	Very High	Medium	High	Confidentiality	Confidentiality Integrity Accountability Auditability	Technical: Dr. must have the right authentication and authorisation based on his role in storing medical health records and safeguarding them with key security regulations.
<i>Description</i> :Risk of hospital staff disclosure of patient confidential information to someone else at the diagnose process.		Sources: Mapped from Enisa 2012 Management interface compromise (manipulation, availability of infrastructure) ISO27799:2008 7.8.1.2 Access control policy The organisation's policy on access control should be established by predefined roles of associated authorities which are consistent with, but limited to, the needs of that role. The access control policy, as a component of the information security policy framework described in 7.2.1 Information security policy document, shall reflect professional, ethical, legal and subject-of-care-related requirements and should take account of the tasks performed by health professionals and the task's workflow.						
The importance of this risk to the healthcare context in Oman		Medium- within Oman, hospital medical staff tend to reveal medical information to family members or a friend without recognising that this action is considered a breach of security. Thus, there is a need to raise awareness regarding disclosing patient information.						

Table 5-2 Sample Row of Updated Risk Register

The Risk Register table was updated after each stage, which resulted in the development of a comprehensive Reference Generic Risk Register ([Appendix C](#)). The Reference Generic Risk Register is one of the contributions of this research.

The Reference Generic Risk Register document includes a range of different risks (46 risks). A sample of management risk is illustrated in [Table 5-3](#), a sample of security risk is presented in [Table 5-4](#), a sample of technical risk is shown in [Table 5-5](#) and a sample of legal risk is demonstrated in [Table 5-6](#).

However, there are limitations related to the generic reference risk register as it lacks visibility due to the size of the risk register table. In addition, it is too generic and high level so it can only be used for reference but not to a specific context. This is a concern as although ODP and ITA-Cloud have expertise in managing information security risks and utilising standards such as ISO 27000, this is not the case in the hospitals. The hospitals therefore need a more effective mechanism to gain a shared awareness of the security risks in their business processes to promote more effective communication of these risks.

No.	Risk Type	Risk Name/ Description	Impact	Likelihood	Risk Level	Risk Perception	Security Goal	Countermeasure
23	Management	Reduced staff productivity.	Gap	Gap	Gap	Technical Competence	Accountability	<i>Human Oriented:</i> Ensure that experts are not dismissed. Involve them in the migration project ,so that they get a sense of ownership. Provide training in cloud technology and enable staff to learn new skills.
		<i>Description</i> During the migration and changes to staff work and jobs, uncertainty leads to low staff self-esteem and nervousness spread in the organisation.						
		The importance of this risk to the healthcare context in Oman	Medium- the move to cloud will be a huge change to the hospital infrastructure. Thus, it needs careful consideration of the time and training needed to put the new system infrastructure in use. This risk has a critical effect on the work productivity as it can reduce the daily achievements by not keeping track on the daily work plan.					

Table 5-3 Sample of Management Risk

No.	Risk Type	Risk Name/Description	Impact	Likelihood	Risk Level	Risk Perception	Security Goal	Countermeasure
11	Security	Data protection risks Ref: Enisa,2012	High Ref: Enisa,20 12	High Ref: Enisa,2012	High Ref: Enisa, 2012	Data Security	Confidentiality Privacy Cryptography	Technical Authorisation Authentication Legal
<i>Description</i> Processing data in another country may experience difficulties regarding data protection legislation. In some cases, it is even considered unlawful by the data protection authority. Ref: Enisa, 2012		Sources: ISO27799:2008 7.12.2.2 Data protection and privacy of personal information In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should manage informational consent of subjects of care. Where possible, informational consent of subjects of care should be obtained before personal health information is e-mailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organization.						
The importance of this risk to the healthcare context in Oman		Low- According to Royal Degree, data stored centrally in Oman. It would be managed by ODP and ITA-Cloud. Thus it reduces the complication of rules and regulation of saving sensitive data abroad. This risk can be high when it moves outside Oman (this will be discussed further in Chapter 6).						

Table 5-4 Sample of Security Risk

No.	Risk Type	Risk Name/Description	Impact	Likelihood	Risk Level	Risk Perception	Security Goal	Countermeasure
41	Technical	<p>Network Breaks <i>Description:</i> Loss of Internet connectivity due to failures at the Cloud Customer's site or the Internet service provider, temporarily reduced network bandwidth on the path between Cloud Customer (CC) and Cloud Provider (CP), and disruptions in the global Internet routing infrastructure leading to the loss of the network path between CC and CP, and failures of the CP's Internet connectivity.</p>	Medium	Medium	Medium	Availability	Availability Integrity	<p>Technical: use multiple cloud providers in different locations to ensure data protection and minimise the loss. This will require additional costs.</p>
		<p>The importance of this risk to the healthcare context in Oman</p>	<p>This depends on the communication speed which is provided by the telecommunication companies as hospitals in the capital might have fibre optic; however, rural hospitals are still using dial-up 56kps which does not work with cloud. Therefore, only hospitals that have fibre optic can use the cloud computing service. and state in the service level agreement the condition of network break.</p>					

Table 5-5 Sample of Technical Risk

No.	Risk Type	Risk Name/Description	Impact	Likelihood	Risk Level	Risk Perception	Security Goal	Countermeasure
43	Legal	Risk from changes of jurisdiction	Medium	Medium	Medium	Out of scope	Gap	Legal: cloud customers need to be fully aware and understand the rules regarding where their data is held (Berry and Reisman, 2012).
Description: the Legal and regulatory framework of where data is held tend to change according to rules and regulation within the custodians country (Berry & Reisman, 2012).								
The importance of risk to the healthcare context in Oman		Low- in Oman, Cloud providers (ODP and ITA-Cloud) hold all the data centrally according to Royal Degree. However, there is a need to set up legal agreement between MoH and ODP or ITA-Cloud in case of communicating with an international hospital.						

Table 5-6 Sample of Legal Risk

Having cloud computing as a motivating example helped to improve the understanding of risks, level of abstraction, security goals as well as creating a risk register with comprehensive countermeasures. It is useful to separate the identified risks into risk management perspectives (Figure 4-2). These are strategic risks, change project risks and operational risks which will be managed differently within an organisation. The risks can be categorised into the following:

- Change project risks associated with introducing cloud computing into the hospital.
- Operational risk associated with central cloud infrastructure managed by ODP and ITA-Cloud.
- Operational risks with the hospital

The scope of this research will focus on operational risks associated with the business process (see Table 5-7). For instance, Identity and Access Management relate to having the right access to the process. On the other hand, Economic Denial of Service is a Central Infrastructure Risk which can affect the entire system within the hospital.

Change Project Risks associated with introducing cloud computing	Operational Level Risks associated with cloud Infrastructure managed by ODP and ITA-Cloud	Operational Level Risks associated with hospital
<ul style="list-style-type: none"> • Loss of Governance • Interoperability Issues • Managing System Deployment • Multi-tenancy • Resource Exhaustion • Reduce staff productivity • Data Lock In 	<ul style="list-style-type: none"> • Economic Denial of Service. • Insecure deletion of data. • Network Breaks • Loss of Backup • Loss of Encryption Key. • Social Engineering Attacks. • Temporary Outages • Data Loss and Leakage • Modifying Network Traffic • Federated Authentication • Physical Intrusion • Software Intrusions • Distributed Denial of Service (DDoS) Attacks. 	<ul style="list-style-type: none"> • Malicious Insider • Identity & Access Management • Third Party access • Lack of ICT skills. • Language Barrier. • Data Protection

Table 5-7 Summary of Different Level Risks

The next section will discuss the main contribution of this thesis, namely Managing the Security Risk-Business Process Model (MSR-BPM) approach as a way to manage security risks within a process. The approach focuses on Security Risks as these were the main area of concern that was discussed in Chapter 3.

5.3 Managing Security Risk-Business Process Model (MSR-BPM) Approach

The limitations of the approach discussed in section 5.2 led to the need to enhance the methodology to ensure the visibility of risks and provide a shared understanding. The researcher applied an enhanced methodology to combine risk register and BPM to create a new approach to manage risks. The proposed approach, Managing Security Risk-Business Process Model (MSR-BPM), combines risk register and business process modelling for managing risks. A risk register documents the assessment of risk with appropriate countermeasures. BPM visualises the risks, activities, roles, security goals and countermeasures in the process models to promote a shared understanding of risks to decision makers and stakeholders. It is important to visualize the risk location in a process or activity level especially when there are different locations involved.

Secure*BPMN (Cherdantseva, 2014) was considered because it uses Business Process Modelling to model security. Secure*BPMN meets the necessary characteristics of security modelling as it features easy-to-learn and easy-to-use graphical Information Assurance Security (IAS) modelling notation, which is accessible by all members of a multidisciplinary team, irrespective of the area of their expertise. It is based on a shared understanding of the IAS domain among the members of a multidisciplinary team. In addition, the semantics of Secure*BPMN is based upon the Reference Model of Information Assurance and Security (RMIAS). RMIAS is based on ISO 27001 and intended for communicating Information Assurance and Security (IAS) concepts to business experts and other non-technical audiences. It reflects a shared understanding of IAS and is, therefore, suitable for an approach to IAS in a multidisciplinary team.

The syntax of Secure*BPMN was designed specifically for human understanding and communication improvement purposes (Cherdantseva, 2014). However, Secure*BPMN did not model risk or discuss the risk management concept.

Secure*BPMN (Cherdantseva, 2014) was extended by adding risk representation to enhance the methodology to explicitly manage information security risks within an organisation. The approach will be based on ISO27005's main Information Security Risk Management processes and combines risk register and business process modelling to Manage Security Risks-Business Process Modelling (MSR-BPM). The emphasis of the MSR-BPM approach is focused on the importance of both documenting the risks and countermeasures in the risk register as well as visualising the whole process in the Business Process Models to identify security risks within every process and activity to enhance shared awareness and understanding of risks. Therefore, it will provide an effective way of visualising and documenting risks with the healthcare processes to help staff have a shared understanding of the identified risk and the appropriate countermeasures associated with their roles in the process.

Some might argue that it may be sufficient to add a risk representation to Secure*BPMN, but this would be missing the risk register. Having a risk register document is a very important element within MSR-BPM approach as it maintains records of the risk name, type, location as well as a suitable countermeasure. It enhances the understanding of risk and maintains a record when a risk is mitigated or modified. Having Secure*BPMN on its own does not really help in understanding the risk, particularly in terms of providing the details of the countermeasure needed in place. Therefore, a risk register is significant as it provides an in-depth analysis of the risk and countermeasure in detail. Also, risk registers are widely adopted in the healthcare domain. Hence, BPMN and risk register are needed to provide a holistic view regarding how to manage risk.

To clarify the contribution of this thesis, a comparison table was created, showing BPMN, Secure*BPMN and MSR-BPM in [Table 5-8](#).

	BPMN	Secure*BPMN	MSR-BPM
Roles	√	As BPMN	As BPMN
Locations	√	As BPMN	As BPMN
Activities	√	As BPMN	As BPMN
In flow	√	As BPMN	As BPMN
Security Goals		√	As Secure*BPMN
Risks			√
Countermeasures		√	As Secure*BPMN
Risk Register			√
Traceability			√

*Table 5-8 Comparison Table between BPMN, Secure*BPMN and MSR-BPM*

Table 5-8 highlights the contribution of this thesis through combining Risk Register and Secure*BPMN to create a new methodology MSR-BPM to visualise risks graphically within business processes. MSR-BPM helps to address the operational risks perspective (see Figure 4-2) through understanding operational risks more holistically as it represents day-to-day operational activities, which include people, processes and information security. Secure*BPMN helps to identify security concerns within processes but it does not explicitly represent risk. The risk register can identify what the risks are and what actions need to be taken. However, it does not include the people and processes needed in place. Therefore, MSR-BPM is an integrated approach which considers the operational risks holistically as it includes a process diagram and risk register.

MSR-BPM represents the link between people, business processes, IT and security concerns as important issues to manage risks. Also, the way of representing the risk within the triangle shape (Figure 5-4) to distinguish different types of risks as security, management, technical, legal and clinical. In addition, MSR-BPM represents the requirements needed to manage risk within the IT system by showing the risk location, creating the risk register and having a traceability column to easily track any changes within the risk identified. This combination of methods emphasises the novelty of

MSR-BPM as an integrated approach to manage risks within a business processes model.

Figure 5-3 illustrates the MSR-BPM approach. Each stage of MSR-BPM will be discussed in more detail in the next section. In addition, the application of the approach will be discussed through a hypothetical scenario in Chapter 6 and then this approach will be evaluated in Chapter 7.

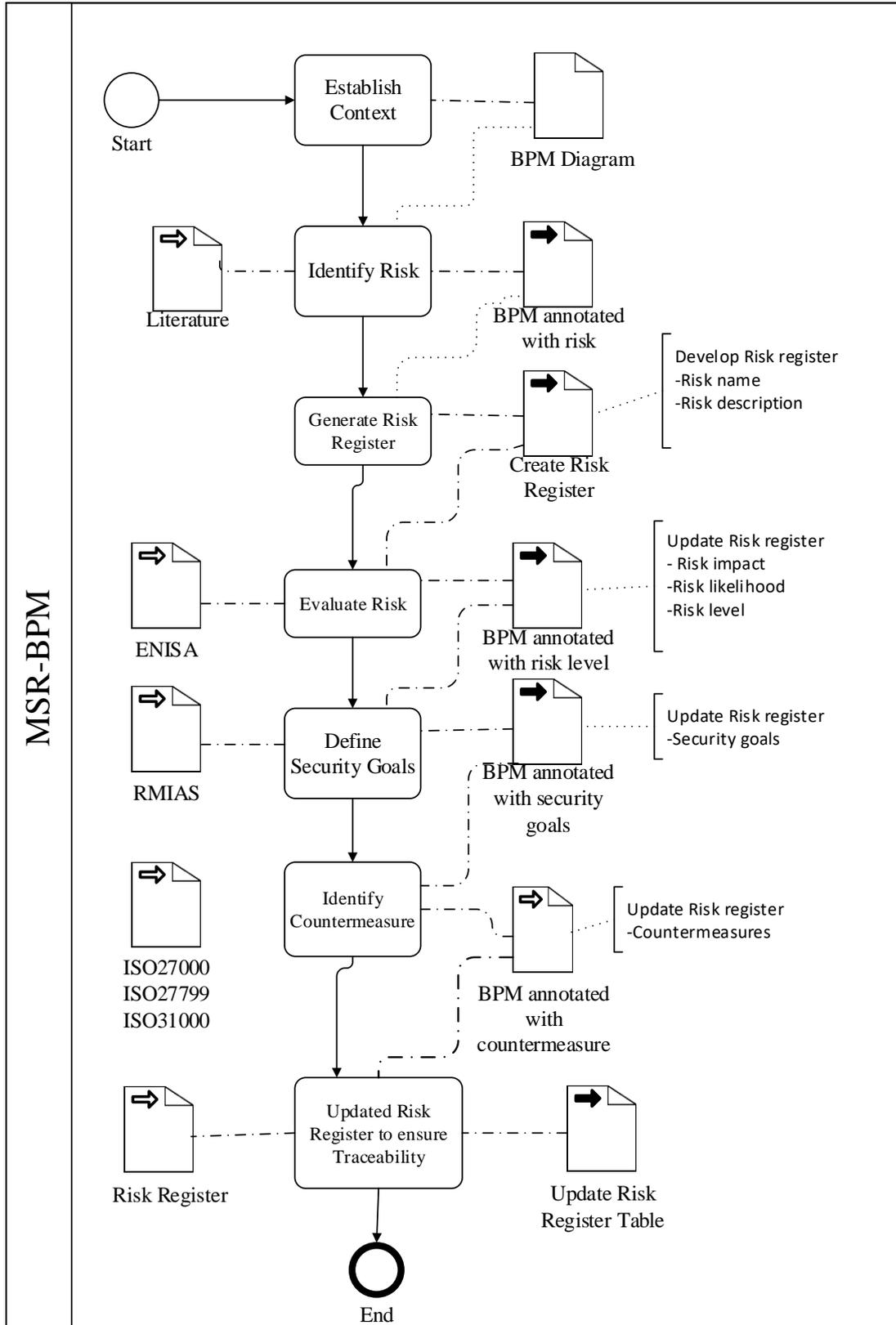


Figure 5-3 MSR- BPM Process

5.3.1 Establish Context

At this stage, it is necessary to understand and represent the workflow within the scenario. Collecting information for the situation being investigated will help in modelling activities and tasks processes within an organisation; it can provide a holistic view of the process. It will show the process involved as well as activities, Swimlane, inflows and locations. In addition, it will help in terms of learning about the artefacts involved, processes, activities, events and location. Creating BPM diagram is important to visualise the whole process. Thus, the output of this stage will be a business process modelling diagram, which will view the current situation with the right level of abstraction and infrastructure.

5.3.2 Identify Risk

Risk identification is a vital stage to determine what could happen to cause a potential loss and to gain insight into how, where and why the loss might occur. It involves the identification of risk sources, events, their causes and their potential consequences (ISO 27005:2011). Secure*BPMN (Cherdantseva, 2014) was used to understand and identify the security requirements. Secure*BPMN helped to deal with security issues at the stage of security requirements engineering and provided a view of security matters in business process models; for instance, access control permission within the different locations. Therefore, MSR-BPM will expand Secure*BPMN by adding risk management to it.

Following a review of the literature (ENISA, 2012; Hosseini, 2013; Mxoli et al., 2014; Latif et al., 2014), various types of risks were identified; security, management; technical and legal risks. These were addressed in the preliminary interview and questionnaire. Further risks were identified to cover clinical risks.

The triangle shape for road hazards was adopted to represent the risk in BPM diagram. Then, Google Search Engine was used using the risk name as a keyword search; [Figure 5-4](#) shows the various types of risk. Figure 5.4a represents security risks with a padlock. Figure 5.4b represents management risk with a human and padlock. Figure

5.4c illustrates the technical risk with a gear. Figure 5.4d identifies legal risk. Figure 5.4e identifies clinical risk. The following shapes in Figure 5-4 are useful to visualise the risk in BPM diagram. It will assist in recognising the risk type and location either in the process or at the activity level.

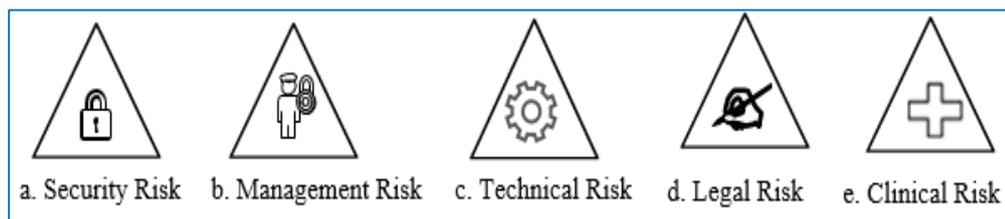


Figure 5-4 Risks Types

This thesis will focus on security risk (Figure 5.4a). Risk types b-e are out of the scope of this research due to time constraints but will be useful to explore in future research. Process models will only include security risks.

5.3.3 Generate Risk Register

By using the literature to identify risk types, a risk register was created to list the risk type, name and a brief description to explain the risk associated with the roles in detail. A sample of a generated risk register is shown in Table 5-9.

No.	Risk Type	Risk Name/Description

Table 5-9 Sample of Risk Register

5.3.4 Risk Evaluation

Risk evaluation is an essential process as it shows the extent to which the vulnerabilities were known, and to understand the nature of risk. With the use of selected methods or approaches, risk evaluation is used to compare the estimated risks against the risk evaluation criteria that were defined during the stage of context establishment to assist in deciding the risk treatment to be undertaken. Decision makers will use risk evaluation criteria to make sure that decisions are consistent with defined external and internal information security risk management context and take into account the objectives of the organisation and stakeholder views. These decisions are mainly based on the acceptable level of risk. However, consequences, likelihood, and the degree of confidence in risk identification and analysis should be considered as well. Risk evaluation uses the understanding of risk obtained by risk analysis to make decisions about future actions. Decisions should include whether an activity should be undertaken and priorities risk treatment according to the estimated levels of risks.

The risk register table will be updated by adding three columns: risk impact, likelihood and risk level. The BPM diagram will be updated by using colours. The MSR-BPM did not adopt the Traffic Light Protocol classification outlined in Jensen et al. (2016), but reproduced it again as in column 4 in [Table 5-10](#) to identify risk level for security risk.

1.Traffic Light Proposal Labels	2.Colour	3.Traffic Light Proposal Classification	4.MSR-BPM Risk Label	5.MSR-BPM Classification Schema
	Red	Highly Sensitive		Red-High Risk
	Amber	Sensitive		Amber-Medium Risk
	Green	Normal Business		Yellow-Low Risk
	White	Public		Green-Opportunity Risk

Table 5-10 Information Classification Scheme

In addition, the perception of risk may change according to the stakeholders' team involved in the discussion as it will be presented through the application scenario in Chapter 6. MSR-BPM approach is useful, as it will visualise the perception of risk in the risk register and BPM diagram.

5.3.5 Define Security Goal

Reference Model of Information Assurance & Security (RMIAS) (Cherdantseva, 2014) was used as an input to define security goals. There are eight security goals adopted from Information Security Management Systems (ISO 27000): Confidentiality, Integrity, Availability, Accountability, Authenticity/Trustworthiness, Auditability, Non-repudiation and Privacy. Information security management in health (ISO 27799:2008) adopted the same security goals as an essential element for healthcare information security. The central purpose of a security goal is to help with

the identification of security countermeasures needed to mitigate threats of a particular type (Cherdantseva, 2014). Therefore, the risk register table was updated by adding a security goals column. The BPM diagram adopted Secure*BPMN notation form to visualise the security goal for each risk. Each risk might have one or more security goals, depending on its type. Table 5-11 shows the updated risk register with security goals.

No.	Risk Type	Risk Name/ Description	Impact	Likelihood	Risk level	Security Goal

Table 5-11 Updated Risk Register with Security Goal

5.3.6 Identify Countermeasure

After evaluating the risk level and security goals, Information Security Management Systems (ISO 27000), Information Security Management in Health (ISO 27799:2008 and 2016) and Risk management standard (ISO 31000) were used to identify the appropriate countermeasures for each risk. Also, the countermeasure symbols defined in Secure*BPMN (Cherdantseva, 2014) were adopted to update BPM diagram with countermeasure symbols. Figure 5-5 represents countermeasure shape and name. The risk register table was updated by adding a countermeasure column.

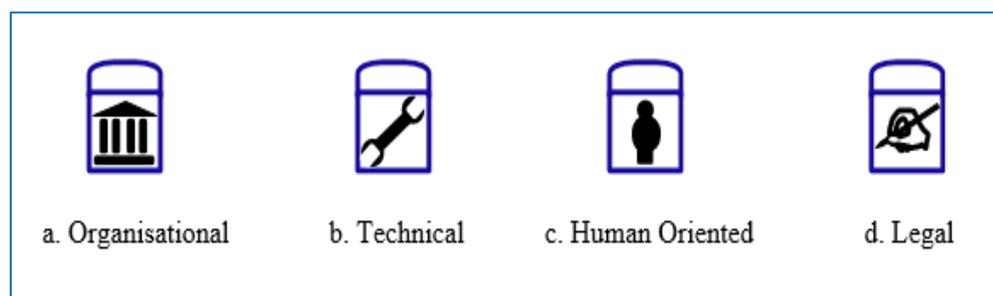


Figure 5-5 Countermeasure Shape and Name

5.3.7 Update Risk Register with Traceability

At this stage, a challenge of tracking the changes in terms of risk persists. For instance, some risks may be classified as low but cause another risk to occur. Thus, it is necessary to locate risk changes easily. As such, a risk register will be used as an input to add a traceability column to facilitate the referencing of risk location, especially when there are different organisations involved. BPM diagram visualises the position of risk, whether it is in a process, activity level or inflow. Section 6.2.7 provides a clear example of an updated risk register with traceability.

Although MSR-BPM helps to provide traceability across the different organisations and disciplines, it does not provide provenance. The concept of provenance is applied to data and information generated within a computer system. The provenance of an item of data is represented in a computer system by some suitable documentation of the process that produced the data, called *process documentation*. This documentation can be complete or partial; it can be accurate or inaccurate; it can present conflicting or consensual views of the actors involved; it can be detailed or not. Provenance is investigated in an open, large-scale systems typically designed using a service-oriented approach (Kifor et al., 2006). Provenance information can be a resource for “reflection-in-action” during analysis, supporting collaboration between analysts, and it can help trace data quality and uncertainty through the analysis process. It can also act as a resource after the event, supporting the interpretation of claims, audit, accountability, and training (Xu et al., 2015).

In healthcare, Agent-oriented cooperation techniques and standardized electronic healthcare record exchange protocols can be used to combine information regarding different facets of a therapy received by a patient from different healthcare providers at different locations. Provenance-awareness enables users to trace how a particular result has been produced by identifying the individual and aggregated services that produced a particular output. This helps users to gain an integrated view of the treatment process executed by distributed autonomous agents, and to be able to carry

out audits of the system to assess whether, for a given patient, the proper decisions were made and the proper procedures were followed (Kifor et al., 2006). However, provenance can be addressed in future research since it is beyond the scope of this research. To some extent, the risk and countermeasures can be expanded broadly as this research did not cover the clinical risks and other elements from a management perspective, which can be added as future research as well. In the current research, the focus is centred on security risks.

MSR-BPM can be adopted within different industries, such as Telecommunications, Banks, and Education, as it is suited to managing complicated processes. When there is a risk within the process, it is hard to show especially when there are multiple organisations involved in the process. MSR-BPM helps to show traceability across different institutions and disciplines, such as in the Integrated Care Pathway (ICP) for breast cancer that will be discussed in Chapter 7 where the MSR-BPM approach is being evaluated.

5.4 Anticipated Benefit of Combining Risk Register with BPM

There are many benefits of combining risk register with business process modelling in MSR-BPM. [Table 5-12](#) illustrates these features in detail.

No	Risk Management Processes	ISO27005:2011 standard Overview	Risk Register Table	Business Process Modelling (BPM)	
1	Establish Context	The external and internal context for information security risk management (ISRM) should be established. This involves setting the basic criteria necessary for information security risk management, defining the scope and boundaries, and establishing an appropriate organisation operating the information security risk management.	Helps to report and communicate risks within an organisation.	Contributes to showing staff roles and location so staff can gain a shared understanding of risk in the process.	
2	Risk Assessment	Risk Identification	Risk identification is to determine what could happen to cause a potential loss and to gain insight into how, where and why the loss might occur. It involves the identification of risk sources, events, their causes and their potential consequences.	Identifies risk name with a short description. Helps to identify risk type Security (S), Management (M), Technical (T) and legal (L) by name.	Identify risk's name in different stages; process, activities and flow dependency. Helps to identify risk type S, M, T and L by symbol.
		Risk Analysis	Risk analysis may be undertaken in varying degrees of detail depending on the criticality of assets, extent of vulnerabilities known, and prior incidents occurring in the organisation. The process comprehends the nature of risk and determines the level of risk.	It identifies risks' level.	It shows different risks' level through colour indication (e.g. red, amber, yellow and green).
		Risk Evaluation	The process of comparing the results of risk analysis with risk criteria to determine whether the risk and its magnitude is acceptable or tolerable.	It identifies Impact and Likelihood.	Does not show.

3	Risk Treatment	Risk Modification	The level of risk should be managed by introducing, removing or altering controls so that the residual risk can be reassessed as being acceptable.	It identifies the countermeasure in detail.	Indicates countermeasure symbol and name.
		Risk Retention (accepting)	The decision on retaining the risk without further action should be taken depending on risk evaluation.		
		Risk Avoidance	The activity or condition that gives rise to the particular risk should be avoided and a process added to effect the treatment.		
		Risk Sharing	The risk should be shared with another party that can most effectively manage the particular risk, depending on risk evaluation and additional risk-mitigation processes inserted.		
4	Monitoring & Review	Risks and their factors (i.e. the value of assets, impacts, threats, vulnerabilities, the likelihood of occurrence) should be monitored and discussed to identify any changes in the context of the organisation at an early stage and to maintain an overview of the complete risk picture.	Update Risk Register to find risks associated with change.	Update process to clearly visualise how risks altered due to change.	
5	Communication and Consultation	Risk communication is an activity to achieve agreement on how to manage risks by exchanging and sharing information about risk between the decision-makers and other stakeholders. The information includes, but is not limited to, the existence, nature, form, likelihood, severity, treatment, and acceptability of risks.		Roles, activities location and storage are shown in model. Gives all parties a shared understanding of risk.	

Table 5-12 Benefits of Using Risk Register with BPM

5.5 Reflection

It was a challenge to use RMIAS to create a Risk Register table because the scope covered all stages in the Security Development Life Cycle (SDLC). The approach is concerned with managing risk so it became necessary to change the SDLC (top left quadrant) to ISMS Processes. In addition, there was the need to change Information Taxonomy Dimension (top right quadrant) to risk information taxonomy in terms of risk identification, risk assessment and risk analysis.

In addition, various challenges were faced in creating the MSR-BPM approach. It was recognised that Secure*BPMN was a strong candidate for modelling security concerns but the process required a lot of research. First, the researcher was unfamiliar with Business Process Modelling technique that represents a vital part in developing the approach. Therefore, Information Technology Object Management Group Business Process Model and Notation (ISO 19510:2013) was studied in order to understand the basic requirements for creating BPMN diagram. If the stakeholders do not have experience in using BPM or the help of an experienced business analyst, then it can be a barrier to adopting MSR-BPM. Therefore, a multi-disciplinary team among the stakeholders is needed to gain a holistic view of risks and capture multiple different perceptions.

Risk Modelling and Risk Register were added as an extension to Secure*BPMN. Then, Dr. Wendy Ivins and Dr. Yulia Cherdantseva were requested to validate the BPM diagram, based on their knowledge and expertise in the area. Confirmation was required from Dr. Yulia Cherdantseva that the extensions were compatible with her approach. Dr. Cherdantseva did not address risk management in RMIAS or Secure*BPM. However, she showed where it is applicable to address in the IAS domain and indicated the requirements for a Risk Analysis methodology which should assist with the creation of a detailed inventory of information and facilitate the prioritisation of security goals. She agreed with the addition of risk representation as an extension to Secure*BPMN. In fact, Dr. Cherdantseva was one of the evaluators of the MSR-BPM approach, in Chapter 7; she provided constructive comments and

positive feedback. She highlighted certain areas for improvements which were incorporated into the methodology presented. The use of a risk register did not feature in her approach.

Difficulties were faced in creating the MSR-BPM approach in the healthcare context, as this was not a familiar area of knowledge and expertise for the researcher. Therefore, there was a close liaison with healthcare practitioners within health centres in Oman. In addition, searching for risk symbols was a challenge as these are intended to be clearly understandable for the general public with different backgrounds. Adopting the triangle shape based on road hazards was the closest option to reality as the general public, whether drivers or pedestrians, are aware of road signs. In terms of the inter-shape, the most applicable and simple symbol was chosen to reflect the risk type as discussed in 5.3.2. MSR-BPM approach can identify new risk categories according to the problem domain. As an example from the healthcare context, the restriction of file access may prevent or delay important information from being disseminated within multi-disciplinary teams meeting in different locations; this will delay the treatment plan for the patient, and, as consequence, it may impact on patients' wellbeing.

The limitation of MSR-BPM approach in the current research is that it does not address the clinical, legal, technical, organisational and environmental risks in detail and this will be addressed in future research. It was identified that clinical risks can be added to the process but the original research did not address this area.

Extensive research was conducted to gain a deeper understanding of the cloud computing domain and healthcare. However, the knowledge and expertise gained was quite limited to a theoretical background only. Therefore, it is important to validate the approach based on the advice of experts in risk management, business process modelling and healthcare.

MSR-BPM approach is useful when there is a complicated process that handles multiple locations and stakeholders because it can identify the risks in each process; this will be evaluated in Chapter 6. Besides, MSR-BPM helps to provide traceability across the different organisations and disciplines, but it does not provide provenance. Provenance in healthcare represents an innovative approach to trace events in complex distributed processes, dependencies between such events, and associated decisions by human actors. Provenance can be addressed as part of future research. Traceability will be revealed in the application of the methodology through a hypothetical case study scenario in Chapter 6.

There are other ways to represent risk register by adding other columns, such as risk ID, risk mitigation action, risk owner, progress in action, risk dependencies and risk status. Organisations should adopt MSR-BPM to fit the way that they represent risk tables in their organisation. However, it is strongly recommended to add a column for risk location within their risk register to easily link the diagram to the table.

The Managing Security Risk-Business Process Modelling (MSR-BPM) approach has been developed to address risks in the context of healthcare. However, it can be broadly used in any industry that would benefit from modelling risks, such as Telecommunications, Education, Banks and Oil and Gas risks. The MSR-BPM approach can provide a shared understanding of risks among stakeholders as well as enhance communication between different locations, as will be explained in detail in Chapter 6.

5.6 Conclusion

Chapter 5 proposed an approach to manage risks by addressing visibility and shared awareness of risk. It introduced using Reference Model of Information Assurance and Security (RMIAS) (Cherdantseva, 2014) to develop a Generic Reference Risk Register Table. It also helped to determine the taxonomy of risk information as risk identification, risk analysis and risk evaluation. A generic reference risk register table

was developed as a contribution of this research that identified forty-six risks from the literature. These risks were categorised as Security, Management, Technical and Legal risks. Also, it used ENISA (2012) as a trusted source to identify the impact, likelihood and risk level for each risk. RMIAS limitations were examined and ISMS processes were used as a basis for developing different approaches. A risk register document was created to provide the assessment of risk with appropriate countermeasures. It also included information about the Omani context and how relevant each risk is to healthcare in Oman. This can serve as a useful reference if Oman decides to adopt cloud computing to enhance the workflow within and between hospitals. Nevertheless, there were limitations related to using risk register alone as it lacks risk visibility within a process.

The methodology was enhanced to represent risks explicitly in business process models. Secure*BPMN (Cherdantseva, 2014) was expanded by adding risk representation to it. The proposed methodology used the main processes in Information Security Risk Management (ISO 27005) as a basis to combine Risk Register (RR) and Business Process Modelling (BPM) to manage security risks. Managing Security Risk-Business Process Modelling (MSR-BPM) approach was used to visualise risks in a healthcare process and promote a shared understanding of these risks for stakeholders.

The anticipated benefits of RR and BPM are listed in [Table 5-12](#) to show the effectiveness of combining them. This will be further explained in Chapter 7. The stages of creating MSR-BPM approach are presented in [Figure 5-3](#) to reveal the different stages in its development.

The MSR-BPM approach was reflected on to explain the challenges in creating the approach. This research purely focuses on security risk; however, MSR-BPM can be broadly used within any industry to show all of the complicated processes involved. Applying MSR-BPM approach is useful to determine risks, especially when multiple organisations are participating in the process. Also, it helps in showing traceability across the different organisations and disciplines, as will be shown in the application of the methodology through a hypothetical case study scenario in Chapter 6.

Chapter 6 will present the application of MSR-BPM approach through a hypothetical case study scenario which was used in the preliminary interviews in Chapter 3. It will illustrate all stages of MSR-BPM in detail. In addition, it will identify the risks in the current situation and in using cloud computing as a solution for enhancing the workflow between two hospitals

6 Chapter 6: Application of The MSR-BPM Methodology

6.1 Introduction

This chapter will introduce the application of the methodology through a hypothetical case study scenario that was used during the preliminary interview in Chapter 3. It will utilise the MSR-BPM approach to visualise risks in a healthcare process and promote a shared understanding of the risks for stakeholders. Each stage of the MSR-BPM will be addressed in two ways. Firstly, the approach used by the author in this research for modelling the scenario will be discussed and, secondly, it will be anticipated how a group of stakeholders might model the approach in practice. In addition, it will identify the risks in the workflow in the current situation and compare the risks in using cloud computing as a solution for enhancing the workflow between two hospitals.

The Ministry of Health (MoH) in Oman are still in the early stages in cloud computing adoption. The ministry uses cloud computing as infrastructure as a service (IaaS) to host the ministry's website in the cloud. Chapter 3 section 3.8 highlighted the perceptions of security concerns of patients' medical records were a key barrier to adopting cloud computing services.

Applying MSR-BPM approach to the hypothetical case study scenario represents a theoretical exercise to prepare Oman for the advent of cloud computing systems into Omani environment in the future. It demonstrates the value of using MSR-BPM approach to identify and manage security risk.

6.2 Hypothetical Case Study Scenario

To examine MSR-BPM approach, a hypothetical case study was used during the interview in Chapter 3. The case study assumes that an *Omani resident (either citizen or expatriate)*, say patient A, suffers from severe headaches and goes to the health centre for treatment. When the doctor diagnoses patient A, he suspects that he is suffering from a head tumour. Therefore, he refers him to a hospital to see a senior

specialist. The senior specialist requests that further investigation is carried out, such as blood test and MRI. The results reveal that the patient suffers from a malignant head tumour and requires an urgent medical procedure, say surgery, to be carried out. The patient decides to travel to a foreign country, say Germany, to carry out the surgery because they are unable to schedule urgent surgery in a suitably short timescale due to a lack of resources in Oman.

If patient A is traveling on government expenses to carry out the surgery abroad, then the foreign treatment department will contact the international hospital on his behalf and send a copy of his medical report via e-mail. If patient A is travelling on his own expenses, then he has to contact the international hospital himself.

Although patient A has a hard copy of his medical report, the international hospital doctor (Germany) is unable to access the medical records stored in Oman's healthcare establishments; thus, the hospital in Germany has to conduct various medical tests and procedures (e.g. x-ray examinations). Unless patient A remains in Germany after the surgery, collaboration and communication between the healthcare workers in both Germany and Oman will be required to provide seamless follow-up post-surgery care. This is not currently possible in the existing Omani healthcare system.

A generic workflow of patient pathway was created to understand the steps in the health centre which can be found in Appendix [D.1](#). Then hospital workflow was developed to understand the processes and activities as shown in [Figure 6-1](#).

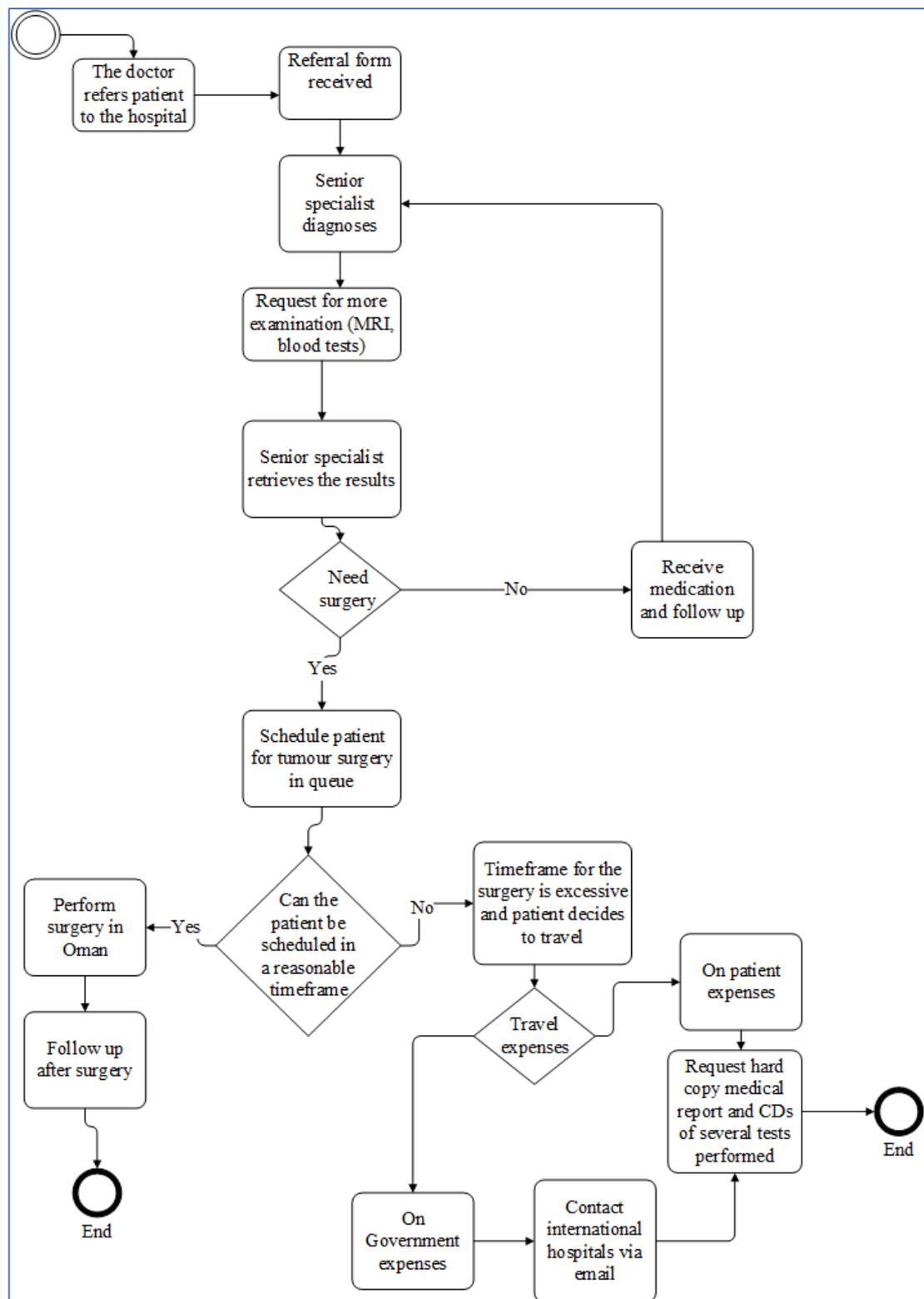


Figure 6-1 Generic Workflow in Oman Hospital

In this research, we will use MSR-BPM approach (as shown in Figure 5-3) to address each stage in *patient A*'s BPM diagram. This will be discussed in two ways: first, how

the scenario was modelled in this research and, secondly, how this could be addressed in practice. To do this, it will be assumed that relevant stakeholders, namely patient representatives, clinicians, Information Technology Authority- Cloud (ITA-Cloud) security analyst, Omani government representative and a representative from the external hosting data centre will work with a business analyst to apply MSR-BPM.

For this research, the focus will be on the surgery performed abroad as the surgery cannot be done within a reasonable time frame in Oman. Therefore, *patient A* will request a hard copy of his medical report as well as a copy of the MRI reported on CD and make travel arrangements to go to the German hospital. He will give this report to the doctor in the German hospital. *Patient A*'s BPM diagram will be presented in [Figure- 6-2](#).

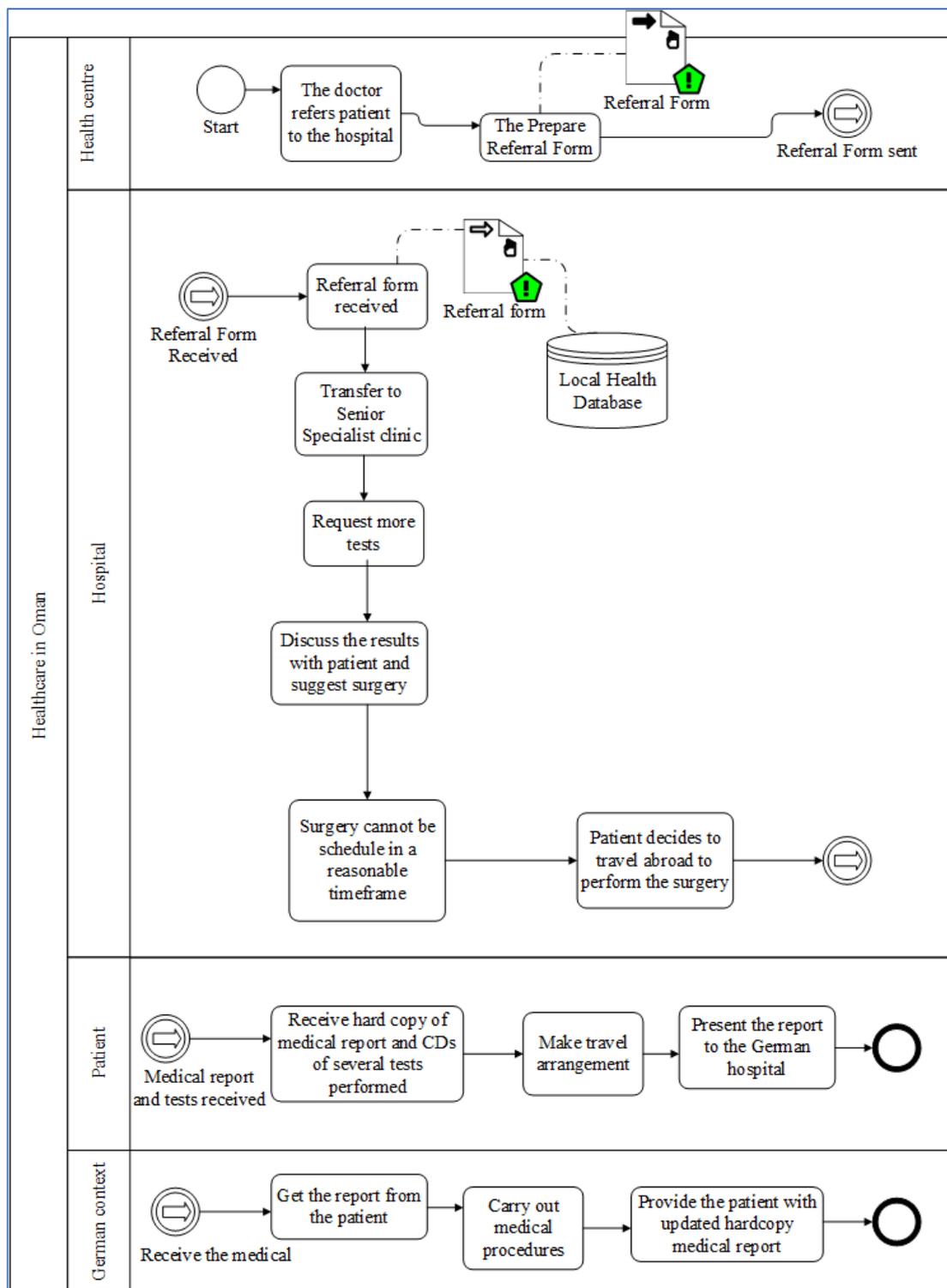


Figure- 6-2 Patient BPM Diagram

The team will gather to discuss the process that the patient has to follow in order to have the surgery performed abroad. Therefore, MSR-BPM steps will proceed as follows.

6.2.1 Establishing the Context

6.2.1.1 Author's Approach

Firstly, it was necessary to establish the context in the healthcare domain. There are commonly used processes for checking the patient. Healthcare professionals cannot create a pathway for every patient, but we are using patient's pathway as an example workflow to help us think through exactly what is happening.

A business process model was developed for patient's pathway in the Oman Hospital. [Figure 6-3](#) illustrates patient's pathway in BPM diagram which was generated from the current process based on the scenario input.

BPM diagram will present the Oman hospital at the process level, and the core activities are; *Referral form received; Transfer to Senior Specialist clinic; Request more tests; Discuss the results with patient and suggest surgery; Surgery cannot be scheduled in a reasonable timeframe and Patient decides to travel abroad to perform the surgery.*

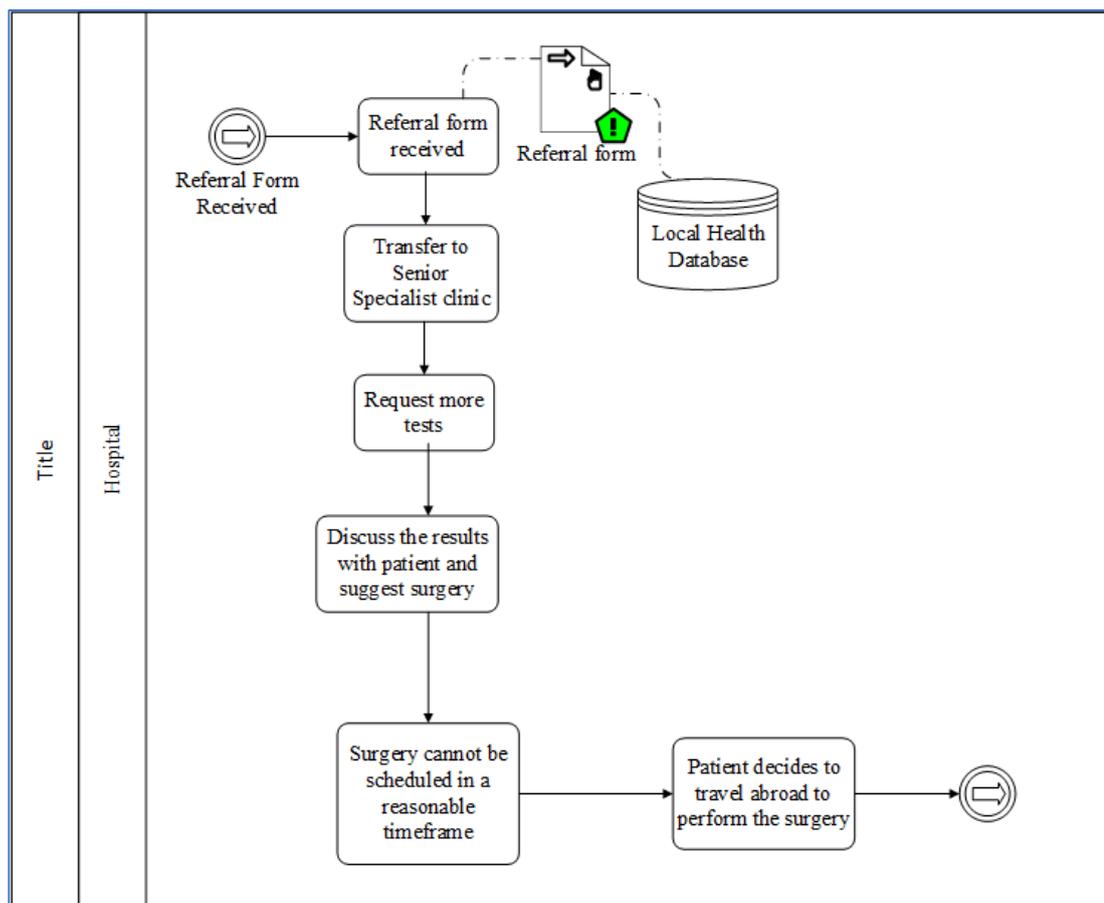


Figure 6-3 Patient's Hospital BPM

6.2.1.2 Consideration for Stakeholder Team of MSR-BPM

In practice, the stakeholder team would not model each patient's pathway independently. However, they can use a scenario such as the one above to help them personalise the process and consider risk for a particular case. The stakeholder team will have different perceptions of patient's pathway and may add different processes or activities based on their knowledge and experience from practice. The stakeholder team may start to identify the risks within the common process. In addition, they need to be careful not to overload the modelling diagram with symbols for every activity.

6.2.2 Identify Risk

6.2.2.1 Author's Approach

Security risks were considered which relate to data security, confidentiality, integrity and availability of patient medical records. The Reference Generic Risk Register Table ([Appendix C](#)) was used to identify the security risks for the hypothetical scenario.

Secure*BPMN was adopted to understand the security requirements within the healthcare context. For instance, who can access the patient healthcare records? Will the patient be able to view his/her medical record online, and what are the threats associated with the process, activity or flow at each stage? The access permission will not be explored in detail in this thesis as it has already been addressed in another research (Burnap et al., 2012; Cherdantseva, 2014).

Malicious insiders were considered as a potential risk within a process level as it can apply to the whole process. An employee who has high access privileges could abuse their role by utilising the granted rights to leak classified and sensitive data. Similarly, safeguarding patient information is applicable for the whole process.

In terms of activity risks, Identity theft risk, was considered in relation to the referral form received. Identity theft means using another person's name and personal information in order to obtain confidential details. For instance, a person might pretend to be the patient to know the status of the referral form without the patient permission which would breach patient confidentiality. In addition, Identity access management risk was considered in Request more tests activity. A doctor might use another username and password to gain access to highly sensitive patient information which is beyond his access roles privileges. Also, Disclosure of patient results risk was identified in Discuss the results with patient and suggest surgery. A nurse might pass the results to the patient without doctor approval which may lead to a critical misunderstanding of the real situation of the patient.

In addition, there are sub system risks such as Insecure deletion of data and System unavailability. The Insecure deletion of data occurs when a patient requests to delete his data from hospital database, they cannot delete the entire disk as it shared by other users too. As for System unavailability risk, there is a possibility of a fault or issue that affects the availability of the hospital systems, and this can be a major issue in an emergency situation where a doctor or nurse needs to access or updated patient information in the database.

The process risks and activity risks were modelled in BPM by creating the triangle shape. The visualisation of risks helps to provide a shared understanding of risks according to the staff roles and responsibilities. Figure 6-4 represents the identified risks.

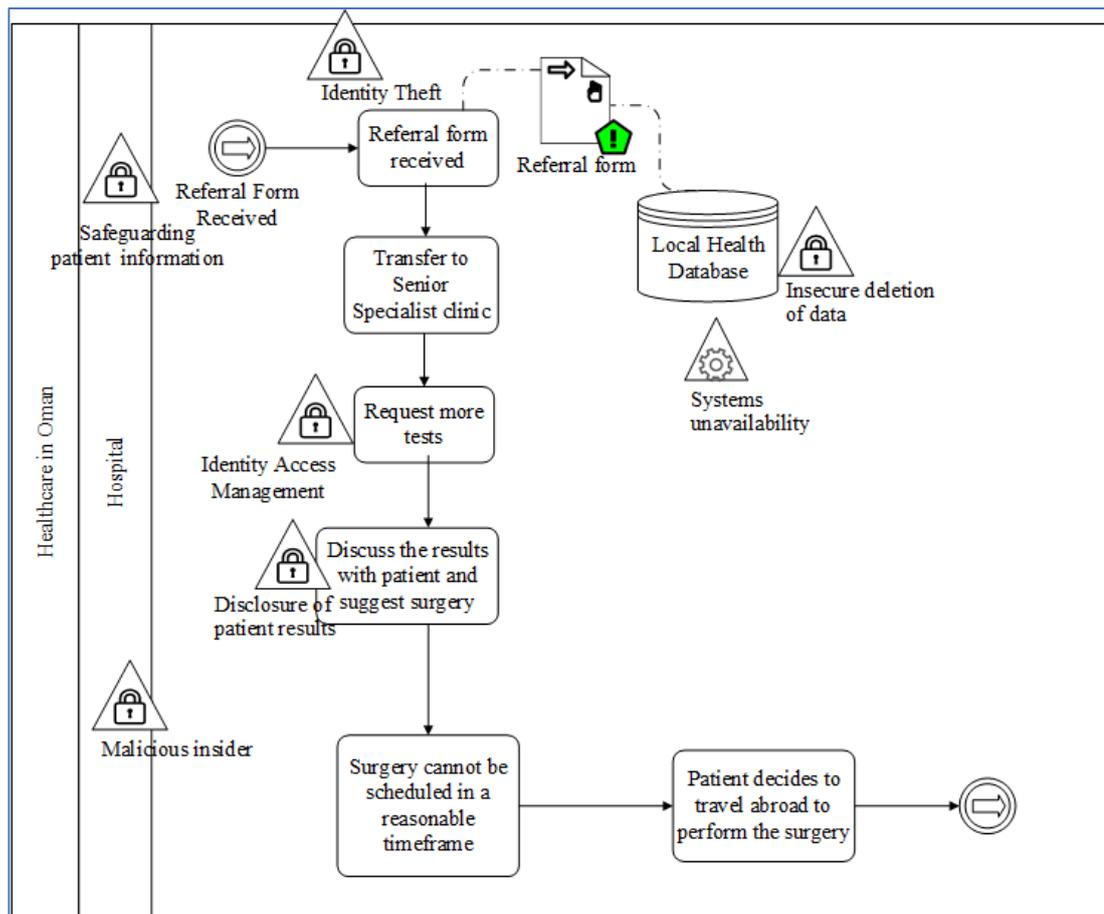


Figure 6-4 Identify Risk in patient's Hospital Process

6.2.2.2 Consideration for Stakeholder Team of MSR-BPM

The stakeholder team will have different perceptions in terms of determining the risks based on their knowledge and experience. The team has to discuss the level of abstraction and access control for all stakeholders involved at every stage. It is a challenge for the team to openly discuss the different opinions regarding access control from the clinician's and the patient representative's point of view. A clinician might not be willing to allow patient medical records to be available online. On the other hand, the patient representative may like to have the medical records accessible online to seek another practitioner's opinion and save unnecessary expenses of re-doing some of the medical tests, such as MRI scans. The explicit modelling of risks encourages the teams to discuss the different options of access control before assigning access permission. Therefore, the team has to assign the access control level for various stakeholders involved in the process according to their role and responsibilities.

6.2.3 Generate Risk Register

6.2.3.1 Author's Approach

At this stage, a risk register table was created (Table 6-1) that lists the risk name and a brief description according to the staff role and responsibilities for the Oman Hospital. The full set of possible risks in the risk register is listed in Appendix [D.3.1](#).

No	Risk Type	Risk Name/ Description
1	Security	Safeguarding Patient A primary investigation health record in Oman Hospital. <i>Description:</i> Safeguarding patient's health record in Oman Hospital with key regulations.
2	Security	Malicious Insider. <i>Description:</i> The risk of staff members in Oman Hospital misusing patient medical information.

Table 6-1 Oman Hospital Risk Register

6.2.3.2 Consideration for Stakeholder Team of MSR-BPM

At this stage, the stakeholder team needs to create risk register table of the identified risks. They have to provide a short description for each risk.

6.2.4 Evaluate Risk

6.2.4.1 Author's Approach

ENISA (2012) was used as guidelines to evaluate the risk impact, likelihood and level of identified risk. For instance, Safeguarding Patient Information will be classified as high-level as it can cause other complications such as disclosure of patient medical data to someone else which violates the patient right to privacy. Malicious Insider Risk will be classified as a high-level risk as it can cause serious damage to the entire process. For instance, accessing records of patients that they are not treating or altering patient data to cover a mistake they have made. [Figure 6-5](#) is updated with security risk level and classified using colours. Also, the risk register table will be updated with the impact, likelihood and risk level. [Table 6-2](#) shows a sample of *patient A's* evaluated risk.

No	Risk Type	Risk Name/ Description	Impact	Likelihood	Risk Level
1	Security	Safeguarding Patient A primary investigation health record in Oman Hospital. <i>Description:</i> Safeguarding <i>patient A's</i> health record in Oman Hospital with key regulations.	Very High	Medium	High
2	Security	Malicious Insider. <i>Description:</i> The risk of staff members in Oman Hospital misusing patient A medical information.	Very High	Medium	High

Table 6-2 Oman Hospital Updated Risk Register with Evaluated Risk

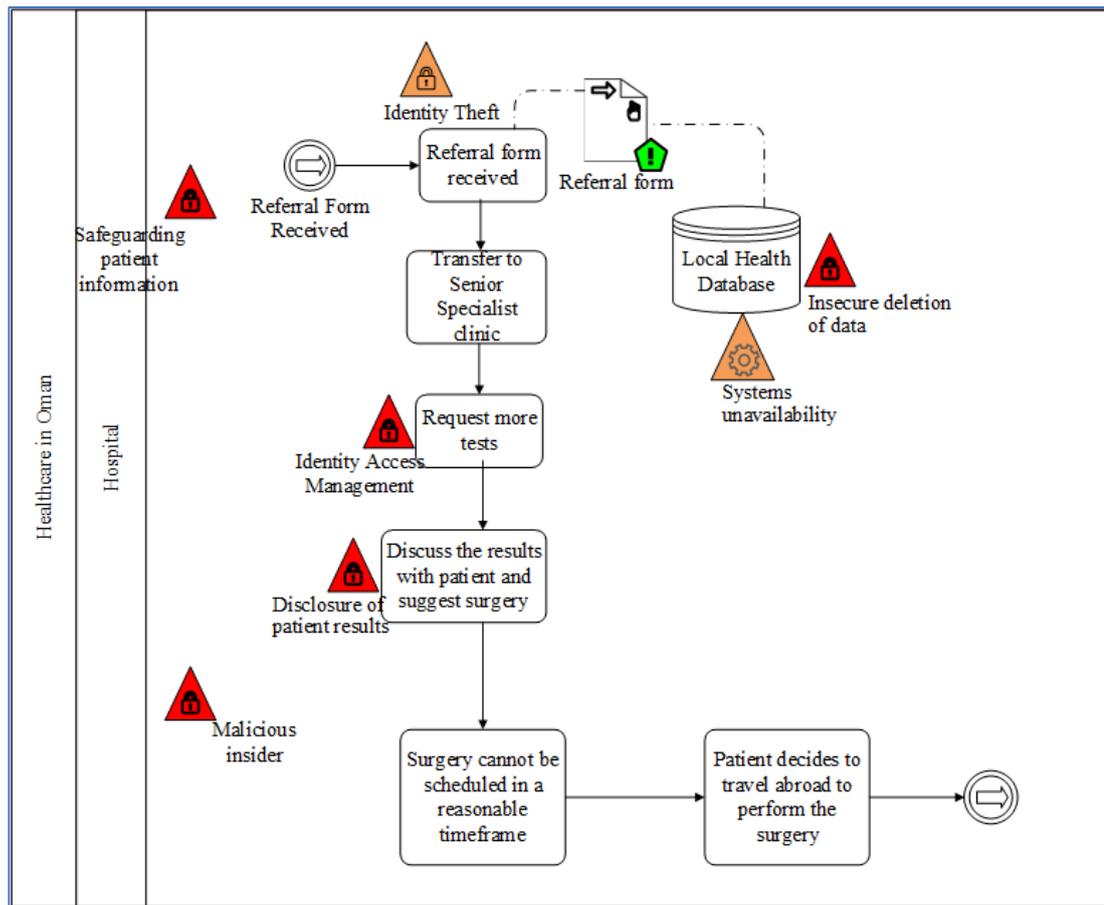


Figure 6-5 Evaluate Risk Level in patient's Hospital Process

6.2.4.2 Consideration for Stakeholder Team of MSR-BPM

The stakeholder team will have a broad discussion to evaluate each risk according to their experience and knowledge. As an ITA security analyst, the malicious insider risk may be classified as medium-level risk because they find a solution such as apply Authorization, Authentication and Auditing (AAA) enforcing strong passwords creation. Only authorised parties are granted access, ensuring that users do not gain access to other users' data for Identity access management risk to reduce the risk level from high within ENISA (2012) to medium. On the other hand, a patient representative might have a different perception and classify the same risk as low based on their confidence in the security measures and practices implemented within healthcare.

A patient representative might emphasise the importance of patients being able to access their medical records online to facilitate the process of having a second opinion and reduce expenses incurred through unnecessary tests. On the contrary, a member of administration from the government may perceive the risk of data protection as high risk, therefore, they will not be willing to upload patient medical records online. Thus, different stakeholders may have different perceptions in terms of evaluating the risk level.

Modelling the whole process may help different stakeholders to reach a shared understanding of risk and come to an agreement. If there is a disagreement, then they will proceed with the higher risk level rather than the low-risk level.

6.2.5 Define Security Goals

6.2.5.1 Author's Approach

At this stage, Reference Model Information Assurance & Security (RMIAS) (Cherdantseva, 2014) was used to identify security goals for each risk. Following RMIAS model is helpful in choosing the appropriate security goal as well as updating the risk register table by adding a security goal column. [Table 6-3](#) presents the updated risk register with security goals.

No	Risk Type	Risk Name/ Description	Impact	Likelihood	Risk Level	Security Goal
1	Security	Safeguarding Patient A primary investigation health record in Oman Hospital. <i>Description:</i> Safeguarding <i>patient's</i> health record in Oman Hospital with key regulations.	Very High	Medium	High	Confidentiality Accountability
2	Security	Malicious Insider. <i>Description:</i> The risk of staff members in Oman Hospital misusing patient medical information.	Very High	Medium	High	Confidentiality Accountability Authenticity & Trustworthiness

Table 6-3 Oman Hospital Updated Risk Register with Security Goals

Figure 6-6 shows the updated BPM diagram for Oman Hospital with security goals. In this research, it emphasises the importance of visualising the risk with security goals to enhance the understanding of risks. In addition, adding the security goals within the risk register table may help in assigning the appropriate countermeasures to mitigate the risks. Therefore, it will be useful to have the security goals in both the risk register and BPM diagram. However, it may add more complexity to the diagram.

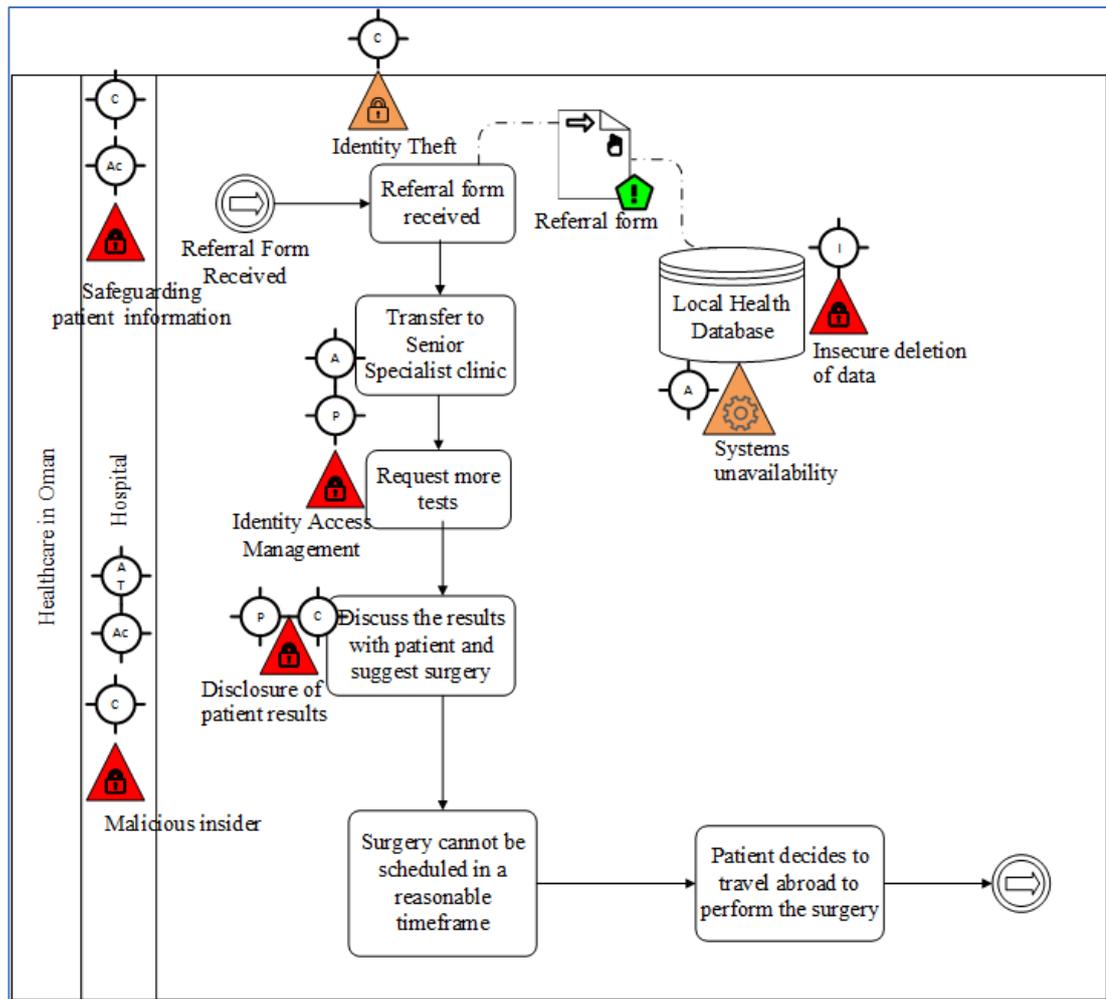


Figure 6-6 Identify Security Goals in patient's Hospital Process

6.2.5.2 Consideration for Stakeholder Team of MSR-BPM

The team discusses the various security goals that they are trying to achieve associated with each risk. The IT analysis expert may take the lead and explain the security goals for the identified risk based on their knowledge and expertise. The discussion about security goals provides an opportunity to place emphasis on what they are trying to achieve and whether the security goals may be usefully added or not to the BPM model.

6.2.6 Identify Countermeasure

6.2.6.1 Author's Approach

Information Security Management in Health (ISO 27799:2008 and 2016), Information Security Management Systems (ISO 27000) and Risk Management (ISO 31000) were used to identify the appropriate countermeasure for each risk in BPM by using Secure*BPMN symbols. It also enhances the risk register table with a detailed explanation of the necessary countermeasures (Figure 6-7). Table 6-4 illustrates Malicious Insider Risk which can have three countermeasures :1) Technical to specify the access control policy for each member in the hospital according to their roles and responsibilities, 2) Human: the hospital must provide security training workshops for all members to enhance their awareness of possible threats, 3) Organisation: the hospital has to notify all members of the security policy implemented

The full set of updated risk register table for Oman Hospital with various countermeasures needed to mitigate the identified risk can be found in Appendix [D.3.1](#).

Risk Name/ Description	Impact	Likelihood	Risk Level	Security goal	Countermeasure
Malicious Insider: <i>Description:</i> The risk of staff members in German Hospital misusing patient medical information.	Very High	Medium	High	Confidentiality Accountability Authenticity & Trustworthiness	Technical: Specify the access control policy for each member in the hospital according to their roles and responsibilities. Human: Hospital must provide security training workshops for all members to enhance their awareness of possible threats. Organisation: Hospital has to notify all members of security policy implemented.

Table 6-4 Patient's Hospital Updated Risk Register with Countermeasures

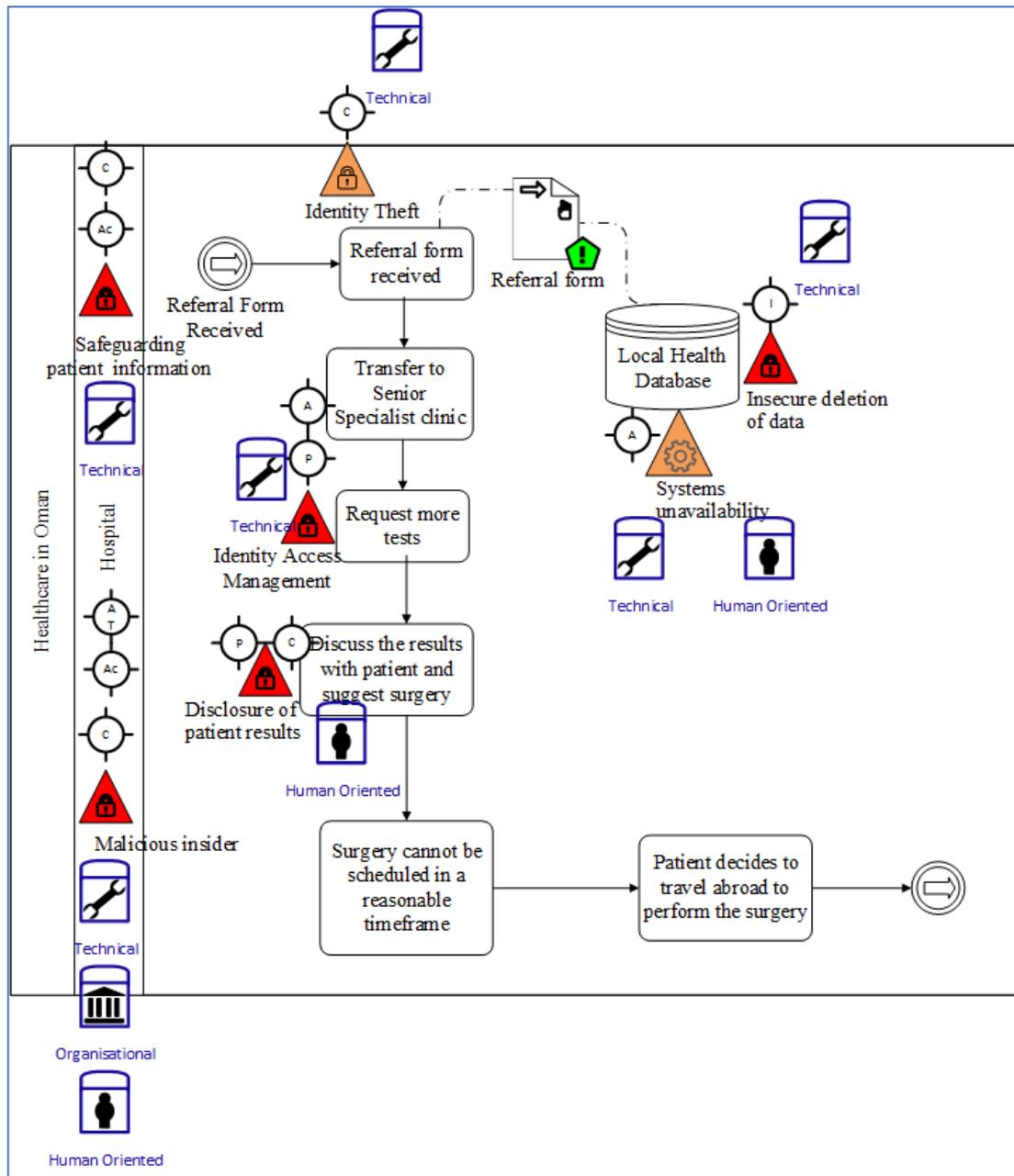


Figure 6-7 Patient's Hospital BPM Updated with Risk Countermeasure

6.2.6.2 Consideration for Stakeholder Team of MSR-BPM

At this stage, the stakeholder team may consider security goals from the previous step to discuss the suitable countermeasures needed for each risk. They will utilise their practical knowledge, such as via an ITA security specialist, in identifying the appropriate countermeasures for each risk. A potential risk may have more than one

countermeasure. For example, a Malicious Insider Risk may have three countermeasures and these may be technical, human and organisational, as shown in Table 6-4.

6.2.7 Updated Risk Register with Traceability

6.2.7.1 Author's Approach

At this stage, the MSR-BPM approach was used to develop the risk register as an input to add an extra column to show traceability, which is not commonly listed in the ordinary risk register table. It is necessary for management at operational level to be able to trace the risk at different locations, especially when there are multiple organisations involved in the whole process. Table 6-5 represents a sample of the risks listed in the Oman Hospital. The full table is available in Appendix [D.3.1](#).

6.2.7.2 Considerations for Stakeholder Team of MSR-BPM

The stakeholder team may consider using MSR-BPM approach as an input to add an extra column for traceability that is useful in operational management to identify any change in these risks.

No	Risk Type	Risk Name/Description	Impact	Likelihood	Risk Level	Security Goal	Countermeasure	Traceability
1	Security	<p>Safeguarding Patient A information</p> <p><i>Description:</i> Safeguarding patient A's health record in Oman Hospital with key regulations</p>	Very High	Medium	High	Confidentiality Accountability	<p>Technical: implementing several layers of authentication such as user login, administration privilege based on their roles and need to access the data to secure health data records adequately.</p>	<p>Oman Hospital</p> <p>Process risk</p>

2	Security	<p>Malicious Insider: <i>Description</i> The risk of staff members in Oman hospital misusing patient medical information</p>	Very High	Medium	High	Confidentiality Accountability Authenticity & Trustworthiness	<p>Technical: specify the access control policy for each member in the hospital according to their roles and responsibilities.</p> <p>Human: hospital must provide security training workshop for all members to enhance their awareness of possible threats.</p> <p>Organisation: hospital has to notify all hospital staff of security rules and regulations implemented in place.</p>	Oman Hospital Process risk
---	----------	---	-----------	--------	------	--	---	-----------------------------------

3	Security	<p>Identity Theft <i>Description:</i> The fraudulent practice of using another person's name and personal information in order to obtain confidential details.</p>	High	Low	Medium	Confidentiality	<p>Technical: authentication based on smart card or certificate. Physical identification and activation required: user finger print. Identity theft requires obtaining the card and the PIN number to access any system. End user must have the liability to ensure his PIN number is protected.</p>	<p>Oman hospital Activity: Referral form received</p>
---	----------	--	------	-----	--------	-----------------	--	---

Table 6-5 Oman Hospital Updated Risk Register with Traceability

6.3 Current situation

In the current healthcare system, as shown in [Figure 6-8](#), there is no cooperation between the Oman and German hospital. Therefore, a patient will need to request a printed report from the Oman hospital before travelling abroad to Germany. The Omani government is currently exploring the extent to which cloud computing could offer a solution. Al Shifa project utilises cloud-computing infrastructure but it does not extend to medical records, as discussed in Chapter 3. There are broad benefits for offering cloud computing as discussed in Chapter 2 section [2.4](#).

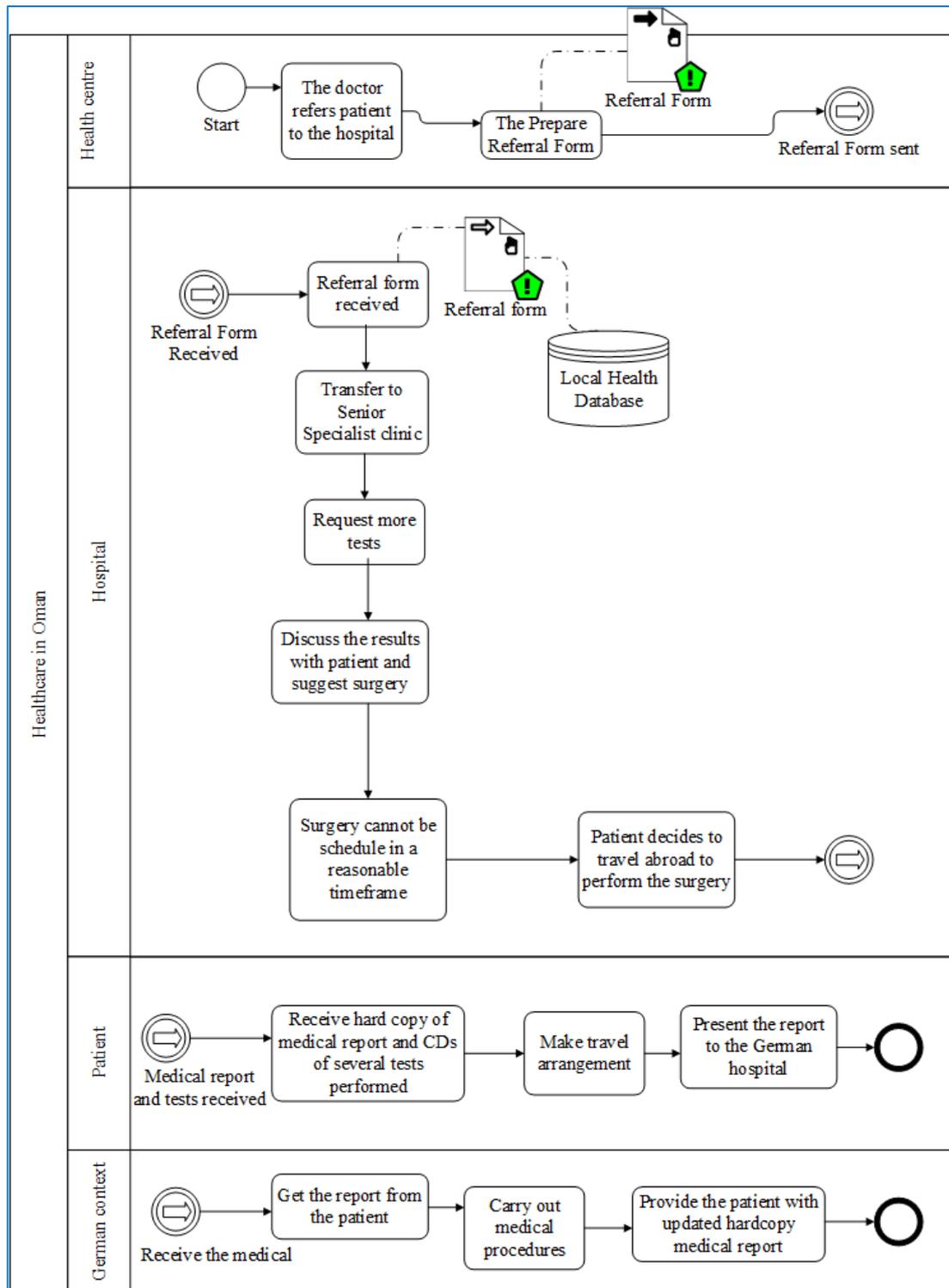


Figure 6-8 Current Situation in Oman Hospital

However, there are various potential risks in this process (as shown in Figure 6-9), such as loss of hard copy report, third party access, not getting the full set of the medical report, data protection, imposter using another patient report. If the patient undergoes surgery in the German hospital, there is no follow-up between the German and Oman hospital to ensure patient wellbeing. It will involve additional risks when following-up patient health or side effects after conducting the surgery. Also, there is a risk of not understanding the language used in the medical reports as it will be written by default in German, whereas it is written in English in the Oman hospital. Appendix D.4 represents BPM for patient process with risk evaluation, security goals and countermeasures. Table 6-6 illustrates possible risks that might occur within the current situation. Therefore, there is the need to have an effective risk management approach to help both patients and clinicians to overcome these risks.

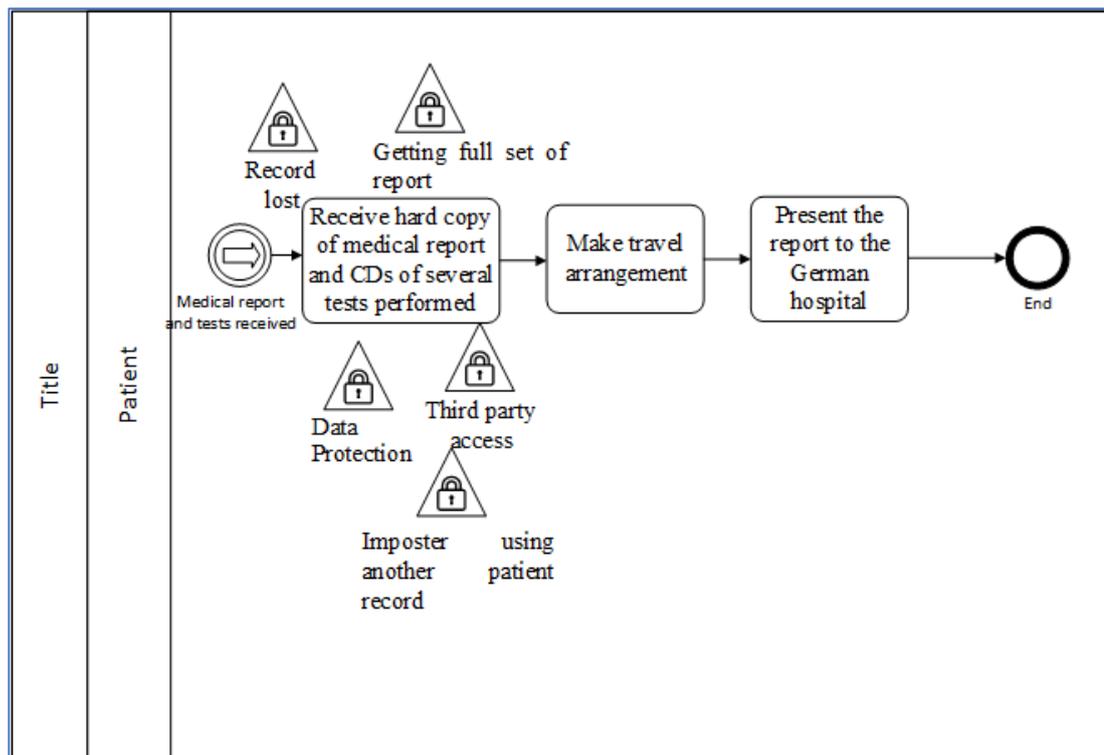


Figure 6-9 Patient Process with Potential Risks

No	Risk Type	Risk Name/Description	Impact	Likelihood	Risk Level	Security Goal	Countermeasure	Traceability
1	Security	Third Party Access <i>Description:</i> there is a risk of third party accessing the hard copy of patient medical report without any permission.	Very High	Very High	Very High	Confidentiality Availability	<i>Human Oriented:</i> patient must secure the hardcopy report in safe bag or in safety box which needs a code to open to avoid any unauthorised access.	Oman Hospital Activity- Receiving hard copy of medical report and CDs of several tests performed
2	Security	Record Could be Lost or Stolen <i>Description:</i> there is a risk of patient losing the hardcopy report.	Medium	Medium	Medium	Availability	<i>Human Oriented:</i> patient A should keep a scanned copy of the hard copy report in their email or in secure flash memory with security code.	Oman Hospital

3	Security	Data Protection: <i>Description:</i> patient needs to secure their hard copy report and CDs of performed results in secure place.	High	High	High	Confidentiality	Human Oriented: patient should keep their record in locked bag and pin code needed to access to avoid unauthorised access.	Oman Hospital
4	Security	Getting the Full Set of Report <i>Description:</i> there is a risk that printer will run out of paper and the printout is not the full set of the report.	Medium	Medium	Medium	Availability	Human Oriented: patient needs to double check the page numbers of report and ensure that they have the full set.	Oman Hospital
5	Security	Imposter Another Patient Record <i>Description:</i> there is a risk of patient collecting another patient report by mistake.	Medium	Medium	Medium	Availability	Human Oriented: patient needs to double check personal details on the report before leaving the hospital to avoid any instance where imposter has used other patient details.	Oman Hospital

Table 6-6 Patient Process Risk Register Table

6.4 Cloud Computing Solution

This section will explore the use of cloud computing as a potential solution to enhance the communication and collaboration between different hospitals. Also, it will enhance access to medical records, improve convenience for patients whilst reducing overall health costs. However, there are risks associated with the adoption of cloud computing as discussed in Chapter 3. From the preliminary interviews conducted in Chapter 3, the main findings from the questionnaires and interviews highlighted concerns relating to data security, confidentiality, integrity and availability, complexity and cost as critical factors preventing the adoption of cloud computing as a service within the healthcare industry. Having secure effective communication is an essential element to consider in order to exchange sensitive data.

The generic risk register helped to identify high- level countermeasures for healthcare context in Oman as discussed in Chapter 5. Many of these risks would be addressed as part of the project to migrate to the cloud computing.

For the scenario mentioned in section 6.2, there is a need for an agreement to be in place between Oman and Germany for exchanging data. It will be assumed that the Oman Hospital (OH) will use one of the two Omani cloud computing providers: Oman Data Park (ODP) or Information Technology Authority - Cloud (ITA-Cloud), both of which are certified by government of Oman (Figure 6-10). The likely infrastructure of cloud computing has been discussed in Chapter 5.

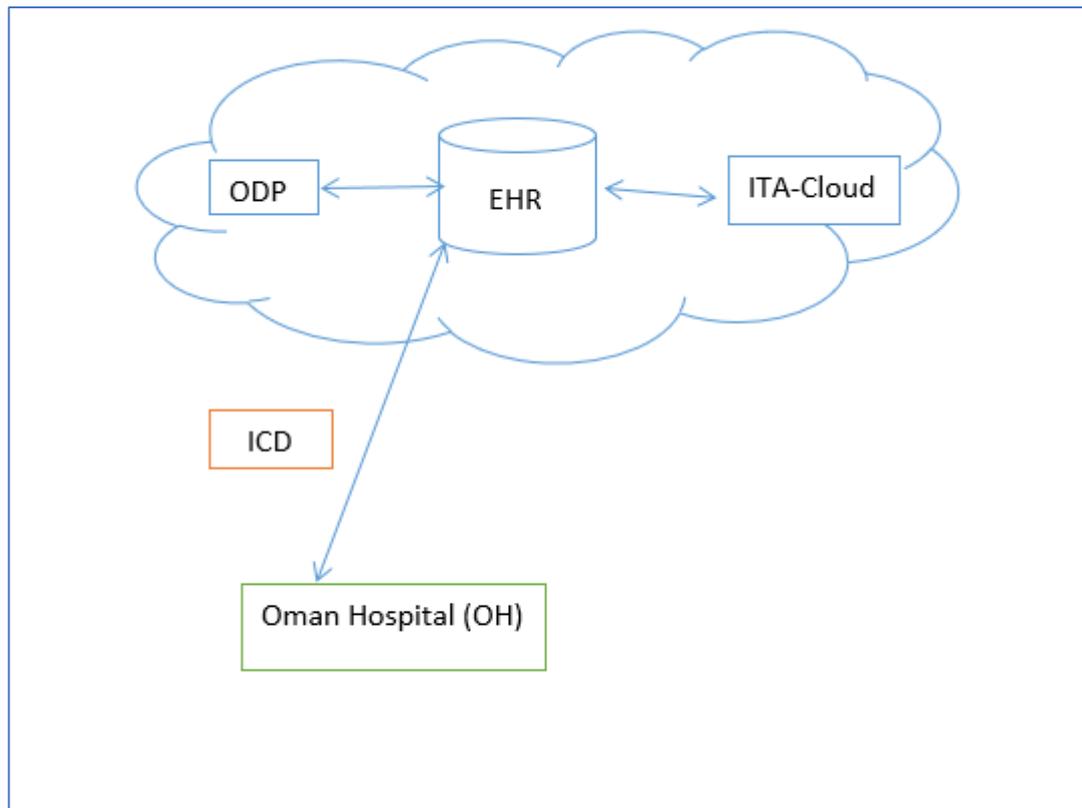


Figure 6-10 Oman Cloud

It will be assumed that the Germany Hospital (GH) uses certified cloud from Germany (Figure 6-11). Cloud provider companies in German follow data protection certificates such as Trusted Cloud data Protection Profile (BSA, 2019). Also, it uses international security standards and certification to protect their cloud services. It incorporates international standards including ISO/IEC 27018, ISO/IEC 27017 and ISO/IEC 27002 (BSA, 2019). The patient and clinician trust will be encouraged to use accredit cloud computing provider services in both countries.

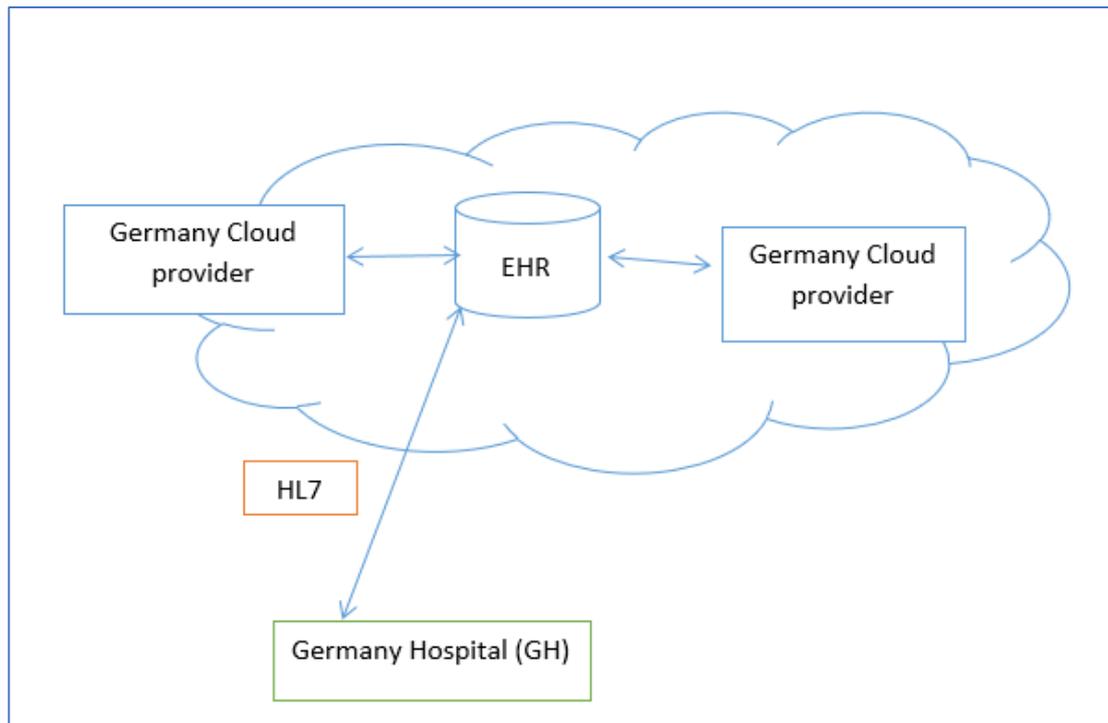


Figure 6-11 Germany Cloud

As for scenario in Chapter 3, the patient decided to travel to Germany for treatment. In Germany Hospital (GH), doctors requested the patient to provide medical history about his case to utilise it with their investigation. Thus, the patient will contact Oman Hospital (OH) to gain access permission for his medical records stored in cloud in Oman.

The Oman Hospital (OH) will contact ODP or ITA-Cloud to gain an access for the patient. ODP or ITA-Cloud will need the patient resident ID number card in order to utilise Primary Key Infrastructure (PKI) service to ensure the true identity of a patient. This will allow a patient to access services which are available on cloud systems by providing authentication and authorisation.

The authentication and authorisation process will be provided through Federation Access Management (FAM). Federated Access provides a secure method of authorisation which uses authentication by the user's own institutional login process. FAM is utilised to allow access for doctors from multiple hospitals to obtain access to networks (e.g Shibboleth). As explained earlier ODP or ITA-Cloud and Germany cloud provider must be certified to host the patient medical records online. ODP or ITA-Cloud is responsible for defining access privilege. In Oman, this was integrated using Oman National Public Key Infrastructure (PKI) either by citizens using their own ID or Mobile tokens to access health services.

After receiving the access to medical records, the patient will share his records with concerned hospital in Germany. [Figure 6-12](#) illustrates the patient pathway within OH to gain permission to access his medical record.

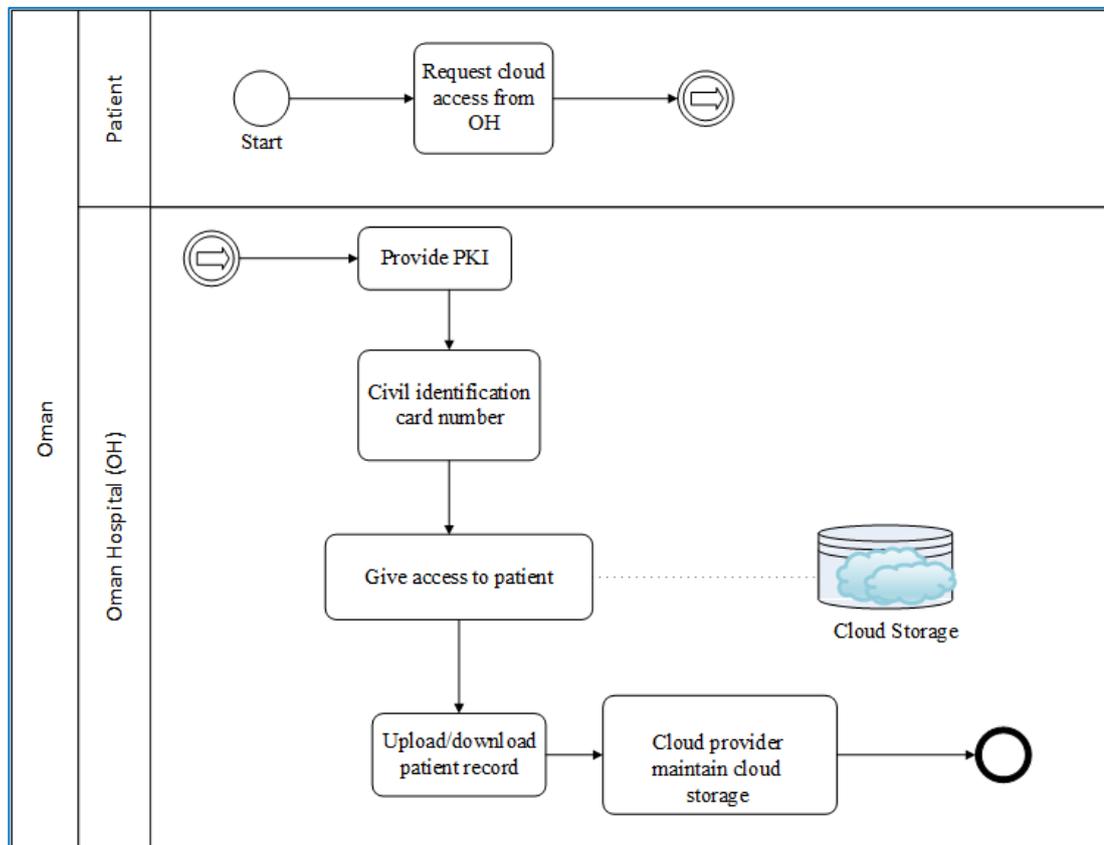


Figure 6-12 Patient pathway within OH for cloud permission

The patient travels to Germany for treatment (Figure 6-13). At GH, doctors will request further examinations. Doctors can view the patient medical records available on cloud hosted in Oman through patient permission access. Then treatment is provided to the patient from GH. The patient requests his medical records to be uploaded to the cloud in order to be accessed for follow up in Oman. Thus, doctors in GH requested an access for the patient from the cloud provider in Germany. The disclosure of patient data will be through authentication and authorisation process.

Upon receiving access to the Germany Hospital (GH), patient allow access to doctors in Oman to view his medical records provided by Germany hospitals for further follow ups.

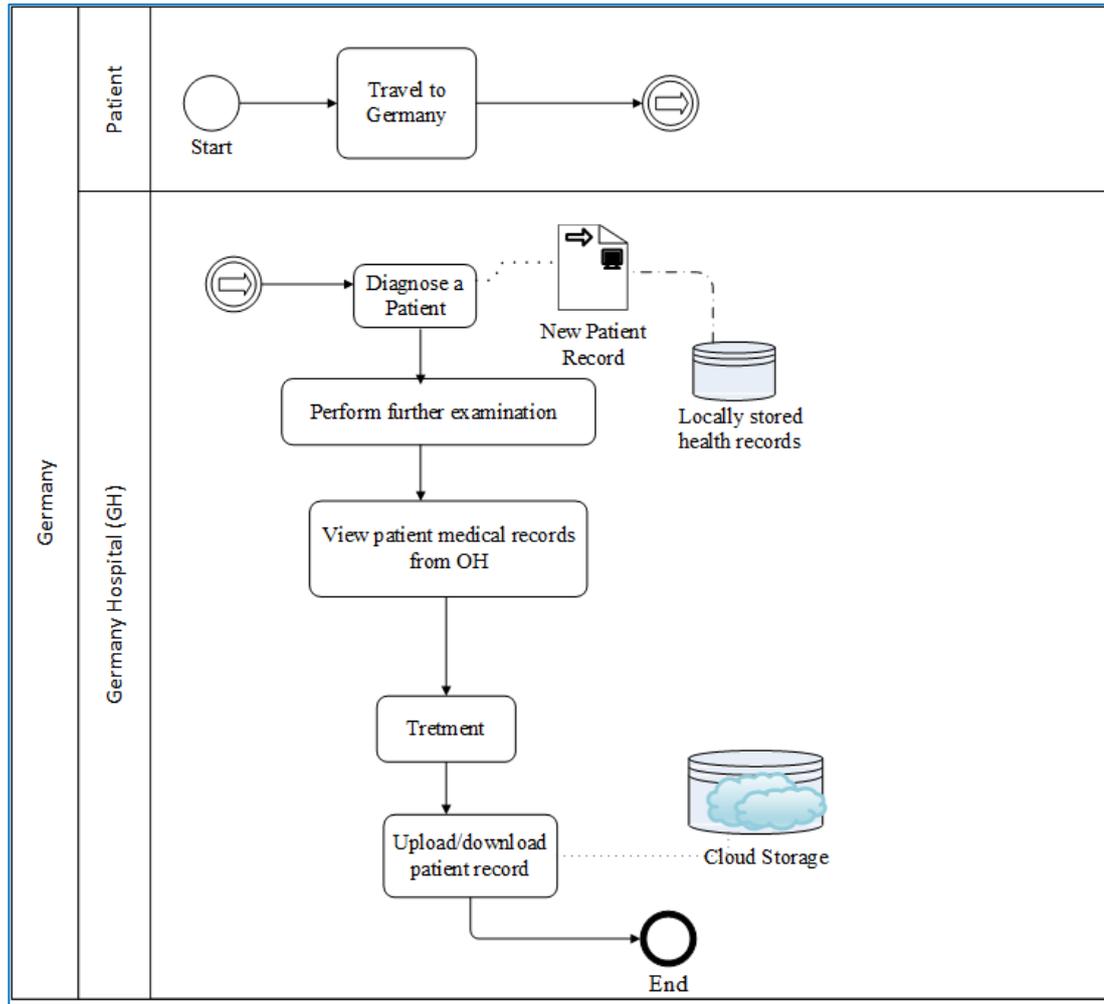


Figure 6-13 Patient Treatment Pathway in Germany

According to risk management perspective discussed in Chapter 4 (Figure 4-2), there are different types of risks in each level which need to be considered. The Strategic level will include the governance strategic plan to set up the procedure for exchanging medical data between Oman and other foreign countries (in this case Germany)

according to the rules and regulations. Different issues may occur such as Risk from changes of jurisdiction because the legal and regulatory framework of where data is held tends to change according to rules and regulation within the different jurisdictions (Berry & Reisman, 2012). Germany will be subject to General Data Protection Regulation (GDPR) rules and regulations and Oman according to Royal Decree. Thus, patient and clinical staff in both countries need to be aware of the changes to the legislation regarding where their data is held (Berry and Reisman, 2012). Another risk can be in IT outsourcing to ODP, ITA-Cloud and Germany cloud provider because transferring health data among various legal and regulatory jurisdictions is absolutely critical and requires a deep understanding of cloud outsourcing contracts (Iyer & Henderson, 2012). Regulations and compliance need to be considered (Seddona and Currie, 2013). There is also a need to provide high level of security with encryption to avoid any leakage during the transferring process.

A risk arises from the need to facilitate Third-party access. Collaboration is needed between MoH in Oman and The Federal Ministry of Health in Germany to exchange patient sensitive data. They need to set up arrangements and measures that must be applied, and agree the service levels to be achieved. The arrangements for compliance auditing of the third parties, and the penalties would also be determined. These will be defined in information exchange agreements that specify the minimum set of controls to be implemented. This is strategic risk managed by MoH.

At project level a key consideration is the Information and Communication Technology (ICT) infrastructure in both countries, and whether they have the right capabilities for the information technology to allow data exchange. Healthcare in Oman currently uses the ICD system to record patients' diagnoses and send ICD messages using the local cloud provider; on the other hand, global hospitals use HL7 to communicate with other healthcare providers. Thus, there is a risk of

interoperability issues between Oman healthcare and international healthcare providers which can affect the availability of records.

The adoption of Health Level 7 version 2.5 by MoH in Oman is recommended to be used to solve the interoperability issue between OH and international healthcare providers. It allows interoperability between electronic health record systems, practice management systems, laboratory IT systems, dietary, pharmacy and billing systems. It serves as a vehicle for different healthcare IT systems, applications and data architectures operating in diverse-system environments to communicate with each other. It is designed to support a central patient care system, as well as a more distributed environment where data resides in departmental systems (International, 2019).

Further project level risks include lack of IS staff knowledge about the importance of migrating to cloud service. IS staff need to have sufficient knowledge, awareness and the required skills to adopt cloud computing (Lian et al., 2014). Therefore, it is important to arrange for training workshop prior the migration process to explain the anticipated benefits for staff to enhance their awareness and understanding. Hospitals in Oman and Germany need to ensure IS infrastructure delivers the right quality of service in terms of technology readiness, existence of the IT infrastructure and human resources. Also, IS complexity and compatibility will affect IT adoption because they need to check the alignments of IT application systems to access the electronic records and applications in both hospitals. Having cloud computing compatibility with existing systems or applications will help make the adoption of cloud computing technology feasible in the hospital.

Also, there are critical projects level risks associated with introducing cloud computing risks that need to be considered such as Loss of governance which can occur by moving to cloud computing service as a hospital will not have full control over their data. Thus, both hospital (OH and GH) will lose control of a system's

infrastructure. Therefore, the hospital's IT department will need to mediate with ODP and ITA-Cloud to negotiate and agree in detail in the Service Level Agreement (SLA) roles and responsibilities before cloud adoption process. To avoid any miscommunication in future. This would specify the exact type of control needed over their data in cloud.

In addition, Reduced staff productivity risk may occur. As the process moves from paperwork to cloud based it will cause reduced staff productivity during the migration and changes to staff work and jobs. Uncertainty can result in low staff self-esteem and nervousness spreading in the organisation. A suggested countermeasure is to ensure that experts are not dismissed and involve them in the migration project so that they get a sense of ownership. In addition, the hospital should provide training in cloud technology and enable staff to learn new skills.

At Operational process level there are risks for day-to-day operation which have been discussed earlier in section 6.2.2. These are Malicious insider, Identity theft and Identity access management. However, when the context changes to security risks in using cloud computing in the healthcare industry there are further operational process risks that need to be considered. Data protection as the patient needs to secure his PKI, whereas in Germany hospital, there is a need for GDPR compliance as patient needs to give consent for accessing his records. Thus, clinical staff need to be trained about the consequences of GDPR in terms of accessing the records and disclosure of patient sensitive information.

In addition, there are operational level risks associated with cloud infrastructure managed by ODP and ITA-Cloud and are applicable for this scenario such as Insecure deletion of data. If patient requests to delete his data from hospital database, cloud provider cannot delete the entire disk as it is shared by other users too. There is also

needed to manage the deletion of data in both hospitals in Oman and Germany as well as data stored about the patient with cloud providers in both countries.

Also, Federated authentication represents delegating authentication to patient A through Oman hospital and Germany Hospital that use Software as a Service (SaaS). ODP or ITA-Cloud would need to provide access to patient to view his medical data in a secure mode in the cloud. The patient will not be able to gain access to other user's data.

Further risk can be in Social engineering attacks if another person attempts to obtain confidential information by pretending to be the patient. Hence, there is a need for Security awareness training for clinical staff to ensure information security of the patient. For instance, the clinical staff need to ask personal questions such as date of birth or address line before providing confidential information.

From this discussion, [Figure 6-14](#) illustrates all those risks and [Table 6-7](#) identifies different risks in detail with suggested countermeasures. In addition, the importance and relevance to healthcare context in Oman is addressed.

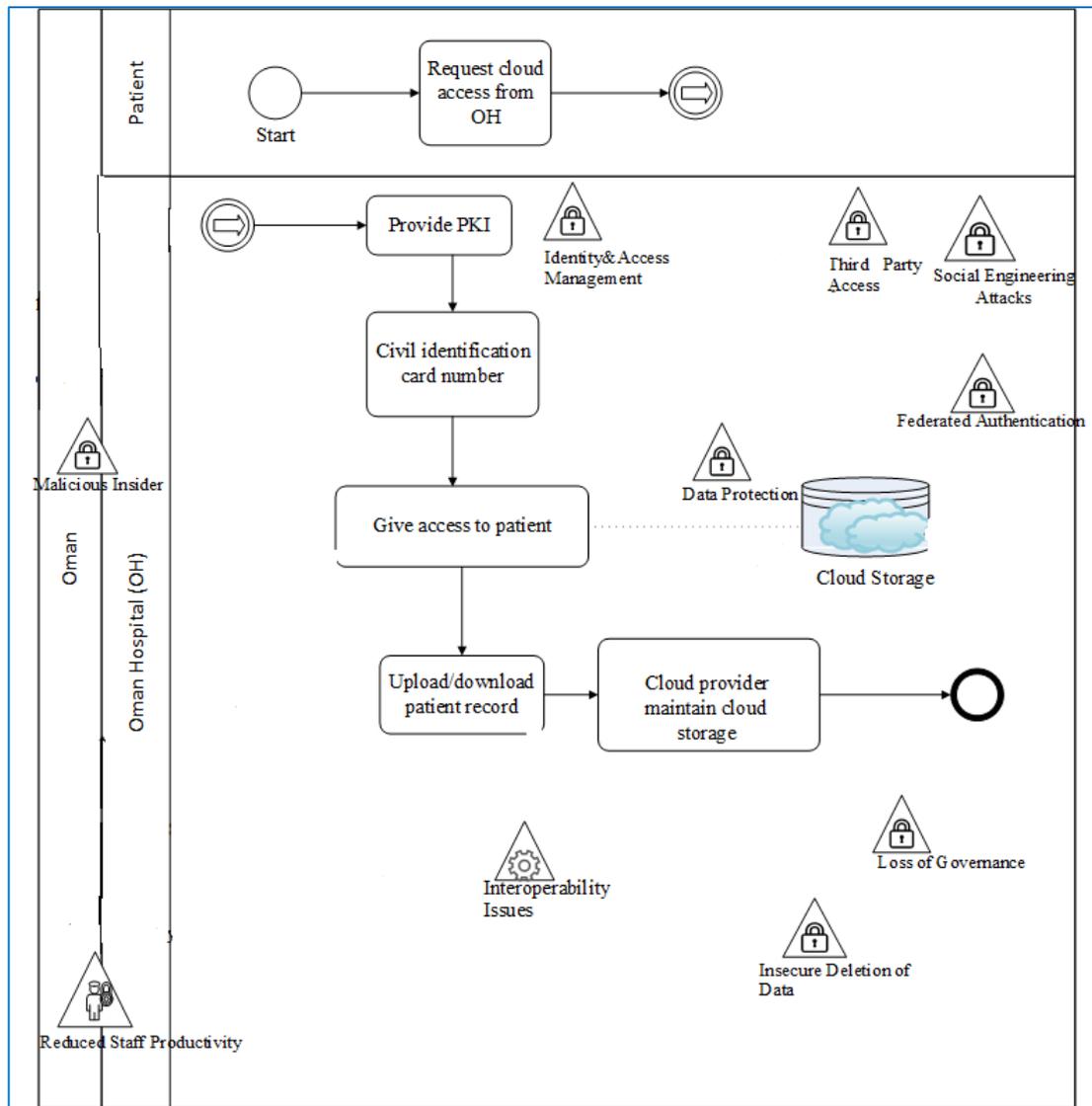


Figure 6-14 Cloud Computing BPM with Risks

No	Risk Type	Risk Description	Impact	Likelihood	Risk Level	Security Goal	Countermeasure	Traceability
1	Security	Data Protection as the <i>patient</i> need to secure his PKI whereas in Germany hospital, there is a need for GDPR compliance as patient needs to give consent for accessing his records.	High	High	High	Data security	<p>Human Oriented patient should keep his PKI safe to avoid unauthorised access.</p> <p>Technical: Doctor and clinical staff need to have access based on their role and they should protect Patient medical information from unauthorized access.</p> <p>Organisational: there is a need for training workshop for clinical staff about the consequence of breaching GDPR rules and regulations to enhance their awareness of security in dealing with patient files.</p>	Oman Hospital Cloud Storage Operational Risk
		How importance this risk to healthcare context in Oman	<p>Low- ODP and ITA-Cloud store the data centrally in Oman according to Royal Degree thus it reduces the complication of rules and regulation of saving sensitive data abroad.</p> <p>As for Germany cloud provider it has to follow GDPR rules and regulations</p>					

2	Security	Insecure Deletion of Data if patient A requests to delete his data from hospital database, cloud provider cannot delete the entire disk as it is shared by other users too. There is need to manage the deletion of data in both hospitals in Oman and Germany.	Very high	Medium	High	Integrity	Legal: signing Service Level Agreement for critical data to destroy data as per user requirement.	Oman Hospital Cloud Storage Strategic risk – setting up SLAs IT Infrastructure risk – managing data deletion
		How importance this risk to healthcare context in Oman	Medium- a ministry need to specify in the service level agreement with ODP and ITA-Cloud the policy for deletion of data and how long for such action can take. The Germany cloud provider has the right measures in place according to GDPR regulations					
3	Security	Identity and Access Management as cloud providers in need to implement security practices to access records as well as supporting privacy guidelines. Thus hospital staff in both hospital will have access according to their roles and responsibility. They are not allowed to access any data beyond their authority.	Very High	Medium	Medium	Confidentiality	Technical: apply Authorization, Authentication and Auditing (AAA) enforcing strong passwords creation. Only authorised parties granted access, ensuring that users do not gain access to other users' data.	Oman hospital Operational process risk

		How importance this risk to healthcare context in Oman	Medium – This is managed by ODP and ITA-Cloud. The Germany cloud provider has the right measures in place according to GDPR regulations.					
4	Security	Third Party Access represents in collaboration is needed between Oman Hospital and Germany Hospital to exchange patient A sensitive data.	Very High	Very High	Very high	Confidentiality Availability	Organisational: MoH in Oman and The Federal Ministry of Health in Germany need to set up an arrangements and measures that must be applied and/complied with for service levels to be achieved. the arrangements for compliance auditing of the third-parties, and the penalties that will apply should any of these not be honoured. Information exchange agreements that specify the minimum set of controls to be implemented must also be used.	Oman Hospital Cloud Storage Strategic risk
		How importance this risk to healthcare context in Oman	Low- ODP and ITA-Cloud hosted the data standalone centrally in Oman. However, MoH will need to sign an agreement with Germany hospital to exchange medical data which will change the impact to Medium level.					

5	Security	Federated Authentication delegating authentication to patient A through Oman hospital and Germany Hospital that use SaaS. A Cloud provider in each hospital can provide access to patient A through the hospital to view his medical data in a secure mode in the cloud.	High	High	High	Confidentiality	Technical: only authorised parties granted access, ensuring that users do not gain access to other users' data. For example, single sign on, federated identity.	Oman Hospital Operational Process risk
		How importance this risk to healthcare context in Oman	High- in Oman authority is given according to the role and responsibility. Thus, patient A can request his PKI from hospital to obtain an access to his medical data. Each hospital needs to ensure that their cloud provider enforces security measures.					
6	Security	Social Engineering Attacks Patient A family members or friends may attempt to obtain confidential information by pretending to be someone else.	High	Medium	Medium	Privacy	Human Oriented: Security awareness training needs to be performed to ensure information security. For all staff within hospitals.	Oman Hospital Operational Process risk
		How importance this risk to healthcare context in Oman	High- in Oman there is lack of awareness of security programs. There is a need for mitigation strategy to deal with those kinds of risks within cloud environment. thus, ODP and ITA-cloud need to provide security training workshop for hospital staff.					

7	Security	Loss of Governance can occur by moving to cloud computing service as a hospital will not have full control over their data. Thus both hospital (OH and GH) will losing control of a system's infrastructure	Medium	Medium	Very high	Data Security	<p>Organisational: Clarify in detail in the Service Level Agreement (SLA) roles and responsibilities before cloud adoption. To avoid any miscommunication in future.</p> <p>Use Service Level agreement to address the exact type of control needed over their data in cloud.</p>	Oman Hospital Strategic risk
		How importance this risk to healthcare context in Oman	Low- according to Oman Data Park (ODP) and Information Technology Authority-Cloud (ITA-Cloud) each Ministry has to sign off service level agreement which indicates the type of control required over their data centre locally and how to act in case of emergency.					
8	Security	Interoperability Issues This is technical risk which causes security risk as healthcare in Oman uses ICD system on the other hand, German hospital uses HL7.	Medium	Medium	High	Data Security Availability	<p>Organisational : Use HL7 version 2.5 to ease the interoperability issues</p>	Oman Hospital Cloud Storage Project risk-migration to HL7
		How importance this risk to healthcare context in Oman	High – Healthcare in Oman currently uses ICD system to record patient diagnoses and sends ICD message using the local cloud provider; on the other hand, global hospitals use HL7 to communicate with other healthcare provider. Thus there is risk of interoperability issues between Oman healthcare and international healthcare provider which can affect the availability of records					

9	Security	Malicious Insider represents the risk of staff members misusing patient medical information.	Very high	Medium	High	Confidentiality Data Security Availability	<p>Technical: specify and implement the access control policy for each member in the organisation according to their roles and responsibilities.</p> <p>Human: organisation must provide security training workshop for all members to enhance their awareness of possible threats.</p> <p>Organisational: Management in each organisation has to notify all members of security policy implemented</p>	Oman Hospital Operational Process Risk
		How importance this risk to healthcare context in Oman	High - this risk is applicable in every organisation as staff members may misuse their work rule in finding unauthorised information.					
10	Management	Reduced staff productivity. As the process move from paper work to cloud based it will cause reduce staff productivity during the migration and changes to staff work and jobs, uncertainty leads to low staff self-esteem and nervousness spreading in the organisation.	Medium	Medium	Medium	Integrity	<p>Human Oriented: Ensure that experts are not dismissed and involve them in the migration project so that they get a sense of ownership. Provide training in cloud technology and enable staff to learn new skills.</p>	Oman Hospital Project Risk

		How importance this risk to healthcare context in Oman	High- the move to cloud will be huge change to hospital infrastructure. Thus, it needs careful consideration about the time and training needed to use new system infrastructure. This risk has critical effect on the work productivity as it can reduce the daily achievement by not keeping track on the daily work plan.
--	--	---	--

Table 6-7 Cloud Computing Risk Register Table

The choice of technology and the erection of governance frameworks to assure security, privacy, availability used to share information across locations has a significant impact on the risks that will be encountered. Having cloud computing as a potential technical solution might facilitate better communication and collaboration between two countries, but it can also raise different types of risks. These risks and associated countermeasures will need to be considered, along with the costs and benefits, when the MoH decides whether they want to extend cloud computing to enable the sharing of patient records.

6.5 Reflection

It was challenging to decide the right level of abstraction based on the scenario input. In the first attempt of modelling (Appendix [D.2](#)), it identified that the patient was suspected to be malignant and required surgery as the only core activities in the Oman hospital. Appendix [D.2.1](#) presented the risk register table for first modelling. It shows similar risks between the Oman and German Hospital. This is unlikely to happen as we do not really know how the German Hospital processes patient data. However, the remodel discussed in [Figure 6-1](#) identified several activities which may occur in the Oman hospital. In addition, the identified risks differ from the first modelling attempt and the current modelling as it identified a wider set of risks. The level of abstraction has a direct impact on the number of risks that are identified. For instance, in the first modelling, the key risks were safeguarding information and malicious insider in Oman hospital. In the remodel, although it identified common risks as safeguarding information, identity and access management and malicious insider, it also identified more risks, such as Identity theft, Identity access management, Disclosure of patient results, Insecure deletion of data and System unavailability.

It is challenging to the extent to which we need to model every process. There are common processes which can be applied to many patient journeys. For instance, the patient pathway may start by checking in with the receptionist and then via the nurse checking blood pressure, weight and height. Afterwards, the patient will be called by

the doctor. It is challenging to include every step the patient goes through, as over time we will have inconsistencies as different multidisciplinary teams have different ideas regarding how the process should be carried out. This may result in having different processes with different activities and there will be different risks encountered as well. It makes more sense to have a subprocess with risks which identify the locations. The use of a subprocess for common process can help us in dealing with both models becoming over complicated and also ensure more consistency when these activities are carried out in different locations. Therefore, the common processes need to be modelled separately.

Although there is a wide range of benefits in adopting cloud computing as a service in health care, the identified list of risks may represent a barrier. Even though we maintained a risk register with suggested countermeasures, there are other types of risks which might occur. As we identify countermeasures, other dependency risks might occur too. For instance, language barrier is considered as a clinical risk, but it can also cause a security risk as more people are involved in a process. If there is a need to use a third party to provide translation, then security risks need to be considered, such as using a certified translator in order to maintain the privacy of the patient record.

There are limitations of MSR-BPM approach in addressing the technical aspect. Multi-tenancy and compartmentalization represent hidden risks that are not visualised easily. However, the cloud provider is required to ensure that consumers may not access other users' information due to multi-tenancy. Cloud service providers should use effective encryption methods to guarantee data isolation between clients. Multi-tenancy and compartmentalization need to be added to the generic reference risk register table. However, those kinds of risks would be addressed by ODP and ITA-Cloud as it will provide the infrastructure and services for accessing the patient information.

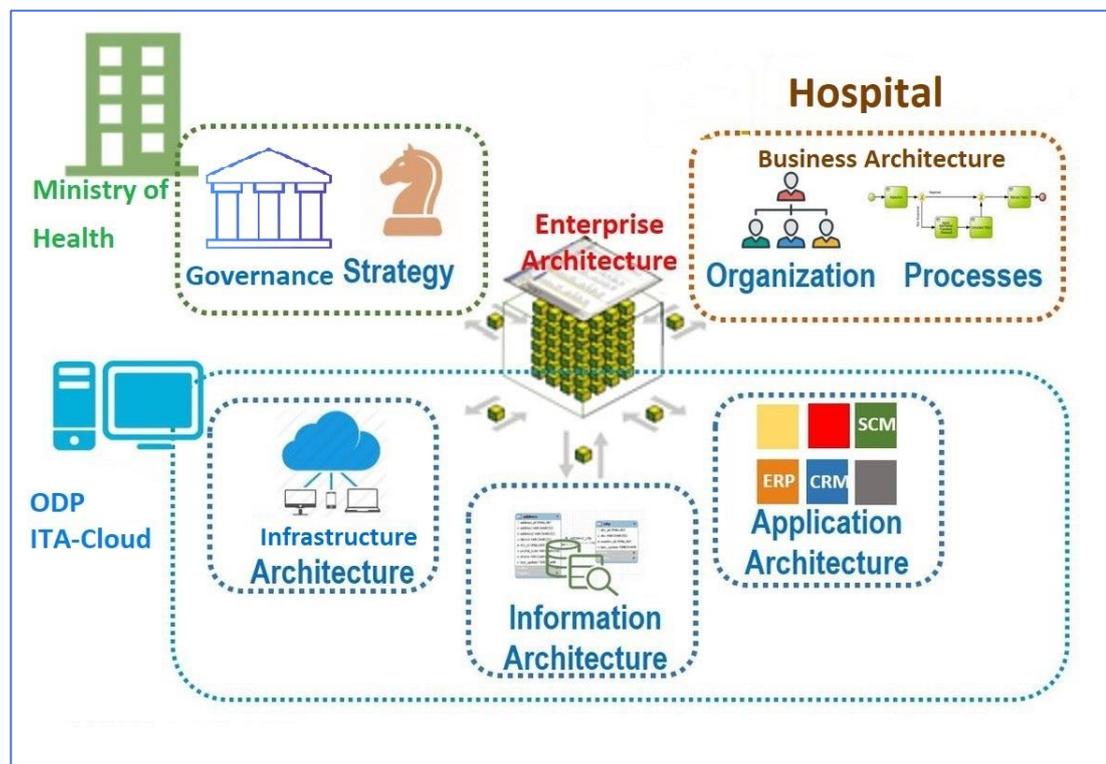
Another challenge related to modelling cloud computing relates to inclusion of the risks of the infrastructure, as the diagram becomes very complex. As the infrastructure

itself is unlikely to change from process to process, it would be preferable to model the human activity workflow separately from its technical aspects. This separation of concerns is a practice used in Enterprise Architecture, where the infrastructure architecture is modelled separately from business architecture. The infrastructure architecture would primarily be the concern of ODP and ITA-Cloud, in close collaboration with the IT staff in the hospitals. Therefore, we did not include the infrastructure aspect in Chapter 7 when we evaluated MSR-BPM approach for the Integrated Care Pathway (ICP) for breast cancer.

If the enterprise architecture approach was used to underpin the migration to cloud then:

- 1) The Ministry of Health would take primary responsibility for governance and strategy.
- 2) ODP and ITA- Cloud would take primary responsibility for infrastructure, information and application architecture so they can migrate hospitals systems and services into the cloud.
- 3) Hospitals would have the primary responsibility to the business architecture and understanding how organisations and process would need to adapt to the migration to the cloud.

This has been illustrated in [Figure 6-15](#).



*Figure 6-15 Enterprise Architecture
Adapted from : (medium.com, 2017)*

There are limitations in using Risk Register and Business Process Modelling as documenting the list of risks tends to grow which will be reflected in the business process modeling by having overcrowded symbols (for example [Figure 6-7](#)) of risks. Hence, there is a need for a multidisciplinary team to have an open discussion regarding which level they need to address the risks in certain situations.

In order to address the complexity in the diagram, it would be better to separate out the different perspective risks: Strategic risks which covers governance aspects, Project risks which handle the migration to cloud computing and Operational risks which covers day-to-day operation in hospital level. This is in addition to separating out the risks with managing the IT Infrastructure, that was discussed earlier.

Figure 6-16 shows the different dimensions that would need to be addressed for managing risks when migrating to the cloud. MSR-BPM approach is primarily focused in identifying security risks in the hospital’s business processes at operational level. However, it does identify some of the risks that will need to be managed at strategic and change project level. Clinical risk is out of the scope of this research but it can be addressed during the modelling process. However, this would need to be addressed in future work. Strategic risks and change project risks can be considered among the future work to expand ISO 31000.

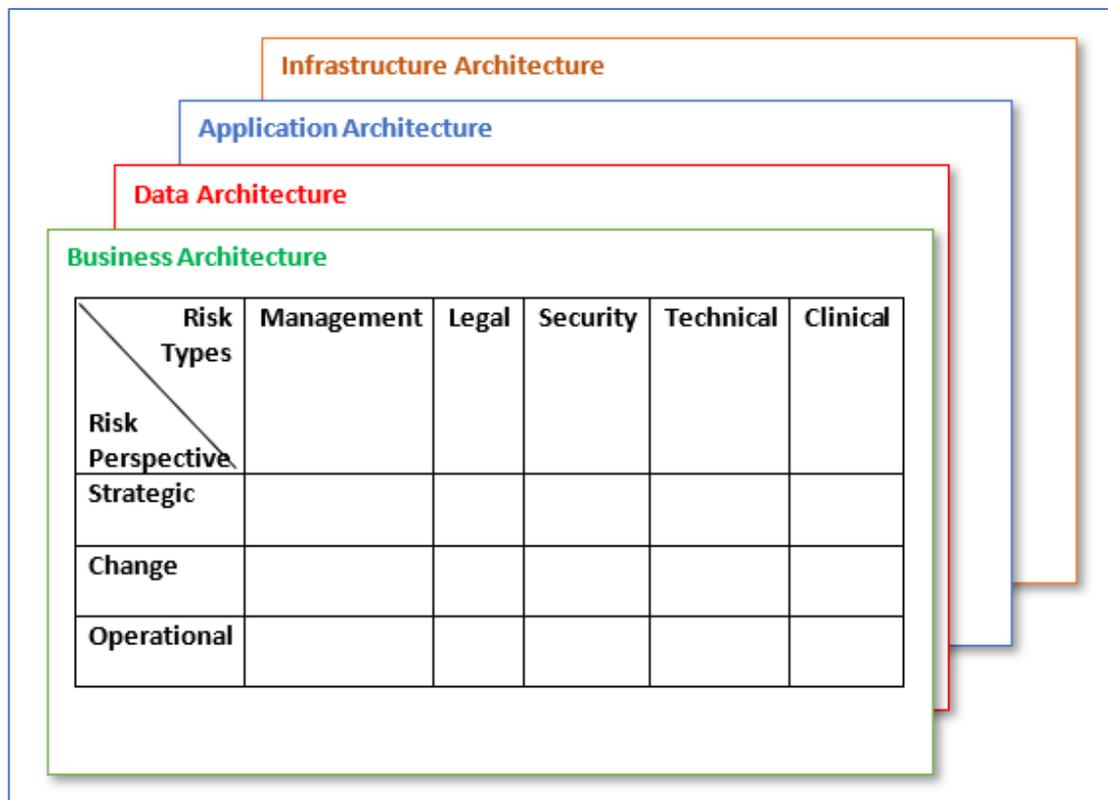


Figure 6-16 Different Dimensions for Managing Risks

Therefore, there is a need for another scenario at operational level which deals with a day-to-day business process to evaluate MSR-BPM integrated approach. It is not possible to evaluate MSR-BPM integrated approach in Oman because risk management are not used within healthcare sector.

6.6 Conclusion

Chapter 6 presented the application of the MSR-BPM methodology and this was considered in two ways; from the author's approach as well as being considered from the potential stakeholder team's response. MSR-BPM stages were applied to the hypothetical scenario, based on Information Security Risk Management (ISO 27005) processes. The risks from prospective stakeholder teams may vary according to their knowledge and expertise in practice. The stakeholder team needs to discuss their perceptions regarding the identified risks based on their knowledge and expertise in the field. There is the need for a multi-disciplinary team to include a business analyst as a stakeholder to ensure the successful implementation of MSR-BPM approach because of BPM's technical terms. Also, an information security practitioner is needed to be able to identify the security risks and suggest countermeasures to address those risks.

It was found that the choice of mechanism used to communicate and transfer medical records between different locations has its own risks. Consideration of risk management perspectives helped to identify different types of risks such as strategic level risks, project level risks which need to be considered as part of the migration to the cloud computing.

The multidisciplinary team will apply MSR-BPM approach to identify the potential risks. The different perception of risks may identify conflicting ideas during the discussion. Therefore, MSR-BPM does not focus solely on representing the risks through BPM, but it also enhances the communication mechanism through the discussion of hidden aspects of identified risks. Consequently, the risks are made explicit and transparent to all stakeholders. Where there are different perceptions of risks, these should be openly discussed when applying the approach.

Chapter 7 will present an evaluation of the MSR-BPM approach using Integrated Care Pathway (ICP) for breast cancer in the UK because it has many potential risks, and the process involves multiple locations as well as various stakeholders. In addition, experts are consulted who have experience in Risk Management, Business Process Modelling and also Healthcare Professionals to validate the MSR-BPM approach.

7 Chapter 7: Framework Evaluation

7.1 Introduction

This chapter will fulfil one of the objectives of this research to evaluate the MSR-BPM approach. It was not possible to make contact with sufficient experts in risk management, business process modelling and healthcare in Oman to validate the approach and therefore it was decided to apply the MSR-BPM approach to a scenario relevant to a UK healthcare context. Therefore, the MSR-BPM approach was applied on an Integrated Care Pathway (ICP) for Breast Cancer. The ICP has been used in various research projects within Computer Science and Informatics at Cardiff University. It has many potential risks which provides opportunities for managing risk because of multiple locations and a range of stakeholders.

Information Security Risk Management (ISO 27005) processes were adopted and a set of software product quality criteria to arrange a set of survey questions for experts who have experience in one or more of Risk Management, Business Process Modelling and Healthcare Professionals. The validation process was done through watching a video for approximately 11 minutes followed by a set of survey questions. The findings were analysed and a reflection on the MSR-BPM approach by highlighting its advantages, limitations and recommendations for future work was provided.

7.2 Comparing MSR-BPM with Other Research Work

There is a need for another scenario to address the operational level risks within a business process. Hence, the Integrated Care Pathway (ICP) for breast cancer was chosen as it shows the processes, roles, activities and different locations. Therefore, ICP for breast cancer represents a realistic scenario to critically evaluate MSR-BPM integrated approach at the operational level within a business process which deals with day-to-day operations. ICP for breast cancer was chosen as it has been evaluated with other research from Computer Science and Informatics at Cardiff University. Although such research used the same Integrated Care Pathway for breast cancer, there are differences in their contributions, and these are outlined as follows:

- Omnia Allam (2006) looked at the communication issues occurring between GPs and members of the cancer care teams. In her research, she created the specification of a system which overcame many of the communication problems by providing a common Electronic Patient Record (EPR) to supply the required information for all the healthcare providers involved. She did not address risk modelling of the communication process.
- Alysia Skilton (2012) proposed a conceptual model which uses care team meta-data to track and manage team members' and professional roles as a means to meet the broader range of requirements of the patient-centric approach beyond the Electronic Patient Record (EPR) held in Cancer Network Information System (CaNISC). She did not address communication or risk in her model.
- Burnap et al. (2012) used the same scenario to discuss access permission between different locations. They presented a system that enhances the way access control technology was deployed so that information owners retain control of their access control and privacy policies, even after information has been shared. However, they did not address risk management or risk modelling within their work.
- Workflow for Integrated Care Pathway (WffICP) (Alsalamah, H 2012) used the automated patient-centric system, but it did not show any visibility of risks within the systems. The proposed WffICP system acts as a central hub for the heterogeneous systems. This means it is not connected into the Clinical Information Systems (CIS) but is used to capture and forward information to and from each of these systems while linking the captured information to create a fuller record for a patient. Therefore, it can inter-operate with different systems independent of their underlying structure, provided a wrapper is provided. The WffICP system acts as a middle layer that lies between the user interface layer and the CIS's interface layer (Alsalamah, H 2012). Therefore, WffICP did not address or visualise risks within the system.

- Secure Healthcare Collaborative Environment (SHarE) (Alsalamah, S. 2014) proposed a broader context of security by providing an information sharing and security context. This approach is a comprehensive and holistic way to address security in collaboration with multiple points of control. It uses BPM in the development of SHarE, which is a successful prototype system. It provides a high-level information security design conceptual model and defines a common collaboration-driven information security goal that meets the needs of information sharing and security contexts in Patient-Centric Care. At the middle level of the security design, it identifies information security threats to this goal and controls that can help address these risks to achieve that goal (Alsalamah, S. 2014). SHarE did not focus on risk management but rather the access control according to the user roles.

The MSR-BPM integrated approach has been expanded from Secure*BPMN to model risk and specify management approach through a risk register. By modelling Integrated Care Pathway for breast cancer, the MSR-BPM can show the risks at an operational level of roles, responsibilities, activities, process and locations in this business process.

7.3 Breast Cancer Treatment Scenario

The importance of using ICP for breast cancer treatment scenario was discussed in section 7.2. The scenario is as follows:

The treatment pathway starts with the patient visiting the GP in a GP surgery after noticing any of the breast cancer symptoms. The GP then examines the patient and collects some information about the abnormality observed, the patient's clinical history, and clinical examination details. This information is stored in the GP's system. If the suspicion of malignancy is negative, then the patient will be discharged. However, if it is positive then the patient is referred to a local hospital (name it Hospital 1) for a breast cancer specialist to conduct further tests. A letter with a summary of the information collected is passed to Hospital 1.

In Hospital 1, an oncologist requests more tests to determine whether the patient has breast cancer or not. These tests include examination (by a Breast Cancer Nurse Specialist), blood test (by a Haematologist), imaging-mammography, ultrasound, and MRI (by a Radiologist), and fine needle aspiration and biopsy (by a Pathologist). The results of these tests (assuming they were carried out in the same hospital) will feed into the oncologist's system to determine the type of cancer, the stage and grade of cancer if the patient was diagnosed with breast cancer. The oncologist should then discuss this thoroughly with the patient and inform the GP.

To plan treatment for the patient, her case is referred to a Multi-Disciplinary Team (MDT) to review for a discussion. Hospital 2 hosts the MDT meetings and must ensure that the information necessary for effective team functioning and clinical decision-making is available at each meeting. Therefore, Hospital 2 requests the patient's information from Hospital 1. The MDT recommends a treatment plan (let us say in this case scenario, surgery was planned for the patient). Then Hospital 2 should inform Hospital 1 about the treatment plan and recommendations and pass on any relevant documents.

If Hospital 1 is the local hospital and does not have sufficient facilities to perform the surgery, then it refers the patient to a better-equipped hospital, Hospital 3, to perform the necessary surgery. This will require that Hospital 1 shares all relevant information of the patient with Hospital 3. In Hospital 3, after surgery, more information will be collected and recorded in the surgeon's system, and a surgery summary will be provided to Hospital 1.

Following the surgery, the patient's case is discussed in another MDT review, and this means Hospital 2 (hosting the meetings) will request all the patient's case notes and reports from both Hospital 1 and Hospital 3, compare it with the previous MDT meeting notes kept at Hospital 2 in order to devise an updated treatment plan and recommendations after the surgery. If the team suggests no further treatment, then the

patient will be discharged and should follow up with the Breast Screening Programme for a regular check-up for any recurrence.

The ICP for breast cancer in UK was used because it is a complex, and realistic process covering multiple locations and stakeholders. The modelling of the central IT infrastructure will be separate from modelling the processes involved. In reality, there are a variety of methods currently in use in both primary and secondary care systems. In the UK, it is typical to communicate with the use of letter correspondence between primary and secondary care. The primary focus is to consider the risks within the complex process. However, when the stakeholder team convene to model a real instance, different perceptions of security risks might be identified based on the team members' roles and expertise.

In this ICP scenario, the focus will be on evaluating the MSR-BPM approach when compared to an ordinary risk register table alone. Risk register is commonly used within UK hospitals, as discussed section 4.7.1.

7.4 Apply MSR-BPM Approach in Integrated Care Pathway

The MSR-BPM approach was applied by establishing the context, identifying risk, generating risk register, evaluating risk, defining security goals, determining countermeasure and updating risk register to ensure traceability.

7.4.1 Establishing the Context

The context used is the integrated care pathway for breast cancer. The BPM diagram was modelled to visualise the whole treatment pathway for the patient in four locations; GP surgery, Hospital 1 for further examination, Hospital 2 for MDT meeting, and Hospital 3 for performing the surgery. The full set of diagrams are available in Appendix [E.1](#). The evaluator will have these sets as an output. As an example, the processes followed by the doctor (Doctor Process) within GP surgery is presented in [Figure 7-1](#).

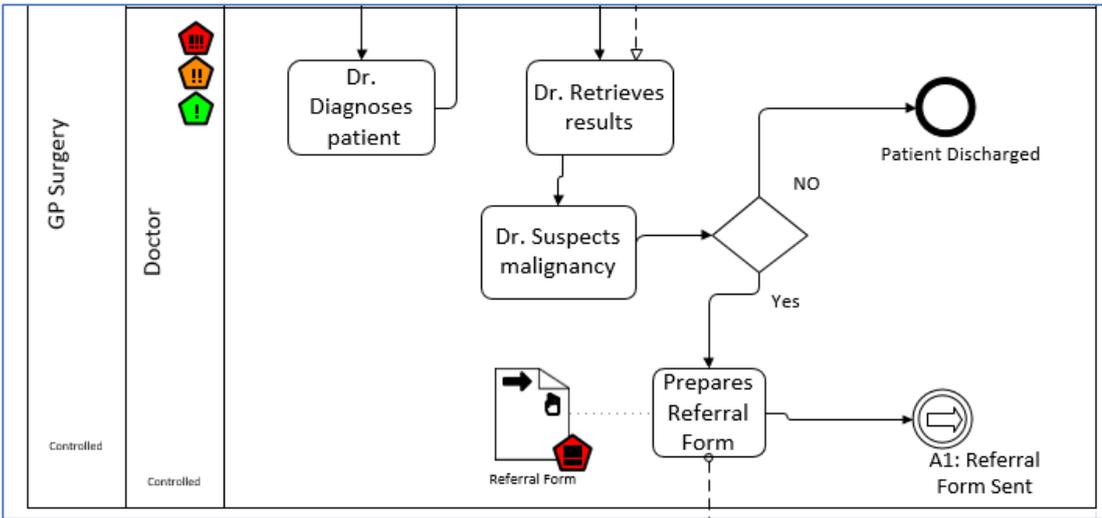


Figure 7-1 Sample of Doctor Process in GP Surgery

7.4.2 Identify Security Risks

Security risks were added to all the process models. As an example of identifying security risks in the GP Referral process, Figure 7-2 illustrates some of the risks in each activity within the Doctor Process.

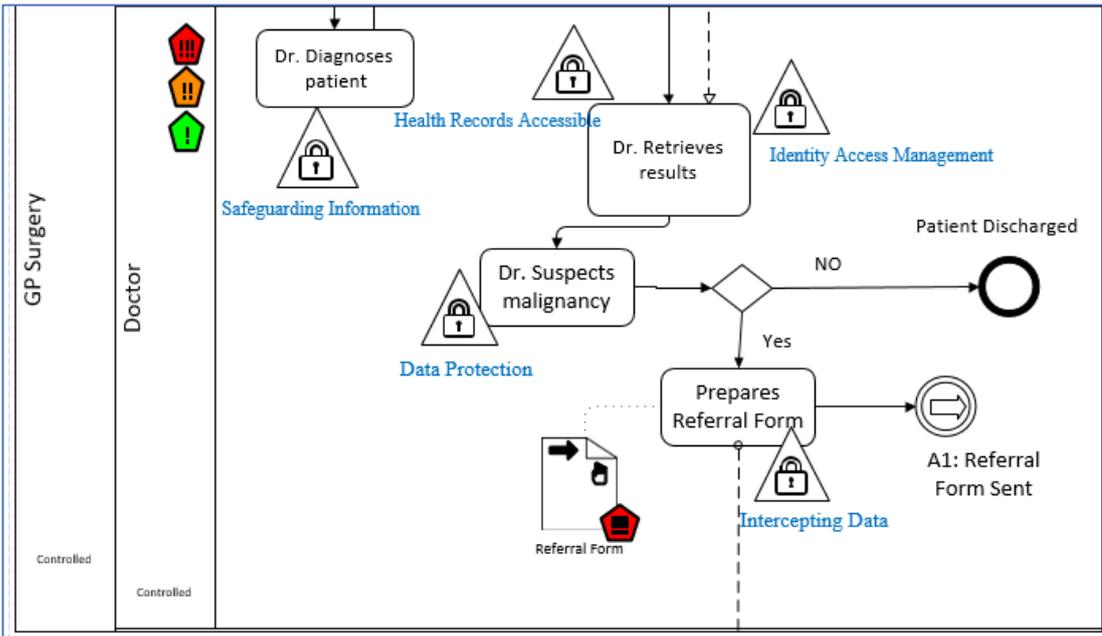


Figure 7-2 Identify Security Risks in Doctor Process

7.4.3 Generate Risk Register

A risk register was generated for four locations to determine the risk's name and description. Appendix [E.3](#) represents the full risk register. A sample of Doctor Process risk register is presented in [Table 7-1](#) below.

No	Risk Type	Risk Name/ Description
4	Security	Safeguarding patient confidential information and compliance. <i>Description:</i> Risk of doctor disclosure of patient confidential information to someone else from the diagnosing process.
6	Security	Health records accessible. <i>Description:</i> The risk of doctor retrieving the results of another patient from health records.
7	Security	Identity Access Management <i>Description:</i> The risk of another doctor using identity and access privilege of another doctor to view the patient's results.
8	Security	Data protection <i>Description:</i> The risk of the doctor sharing suspicions of malignancy based on results with another person without the patient's approval.
9	Security	Intercepting data in transit <i>Description:</i> The risk of disclosure from a doctor or nurse when processing the referral form between different places, computers or sites.

Table 7-1 Sample of Doctor Process Risk Register

7.4.4 Evaluate Risk

To evaluate the risk level, a risk register was used as an input. In addition, the ENISA (2012) was used to identify the impact, likelihood and level of the risk. The risk register table was then updated by adding three columns that resemble each of them (impact, likelihood and level of risk). This information is important to assess the treatment of risk, whether it is cost-effective to be mitigated or whether it can be minimised. [Figure 7-3](#) represents the risk evaluation for part of the GP Referral stage in the process.

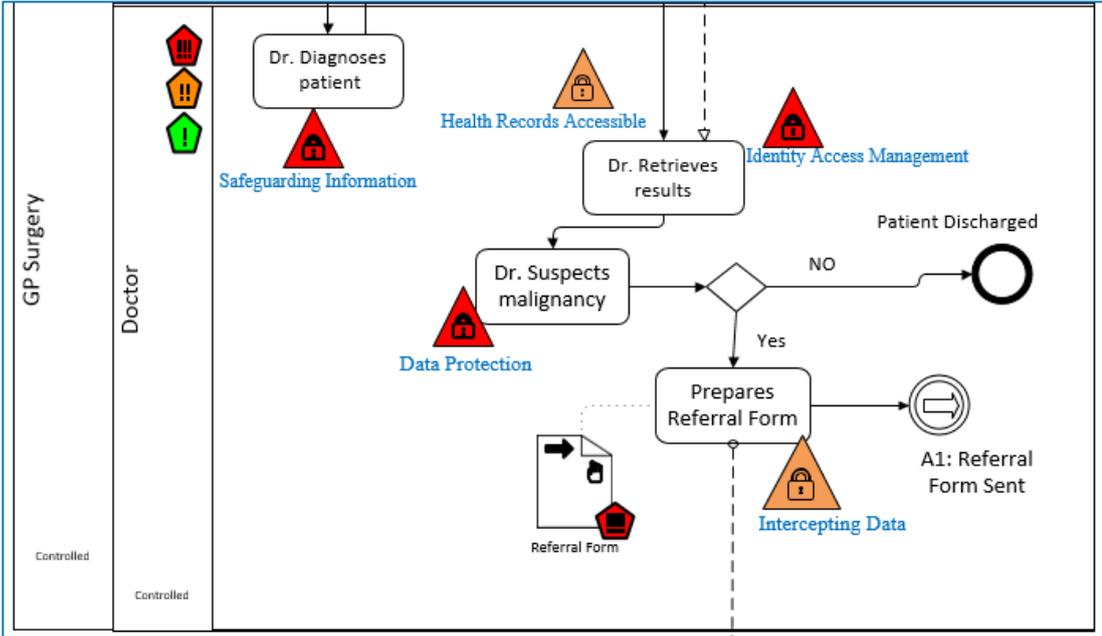


Figure 7-3 Risk Evaluation

A sample of the updated risk register with risk evaluation is presented in Table 7-2.

No	Risk Type	Risk Name/ Description	Impact	Likelihood	Risk Level
4	Security	Safeguarding the patient's confidential information and compliance. <i>Description:</i> Risk of doctor disclosure of the patient's confidential information to someone else from the diagnosing process.	Very High	Medium	High
6	Security	Health records accessible. <i>Description:</i> The risk of doctor retrieving the results of another patient from medical records.	Very High	Medium	High
7	Security	Identity Access Management. <i>Description:</i> The risk of another doctor using identity and access privilege of another doctor to view the patient's results.	High	Low	Medium
8	Security	Data protection. <i>Description:</i> The risk of doctor sharing suspicions of malignancy based on results with another person without the patient's approval.	High	High	High
9	Security	Intercepting data in transit. <i>Description:</i> The risk of disclosure from a doctor or nurse when processing the referral form between different places, computers or sites.	High	Medium	Medium

Table 7-2 Sample of Doctor Process Risk Register-Evaluation

7.4.5 Define Security Goal

RMIAS (Cherdantseva, 2014) was adopted at this stage to specify the security goals to maintain in each activity. Figure 7-4 represents the updated BPM diagram part of the GP Referral in the Doctor Process. The risk register table was then updated by adding a security goal column.

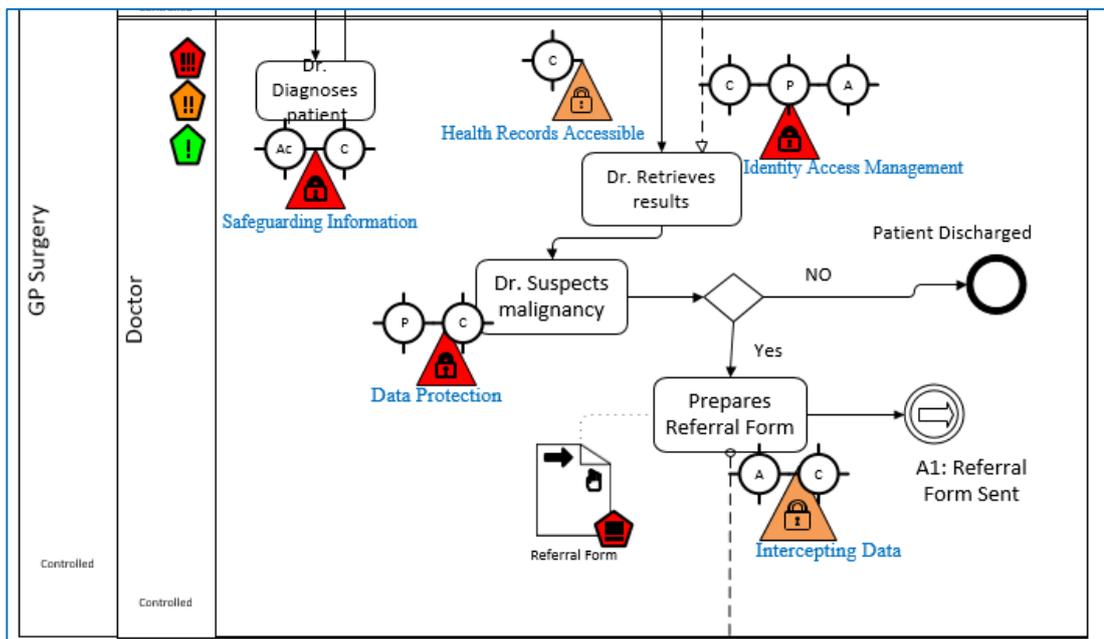


Figure 7-4 Evaluate Security Risks in Doctor Process

The updated risk register Table 7-3 will present the security goal for each risk.

No	Risk Type	Risk Name/Description	Impact	Likelihood	Risk Level	Security Goals
4	Security	Safeguarding the patient's confidential information and compliance. <i>Description:</i> Risk of doctor disclosure of the patient's confidential information to someone else from the diagnosing process.	Very High	Medium	High	Accountability Confidentiality
6	Security	Health records accessible. <i>Description:</i> The risk of doctor retrieving the results of another patient from medical records.	Very High	Medium	High	Confidentiality
7	Security	Identity Access Management. <i>Description:</i> The risk of another doctor using identity and access privilege of another doctor to view the patient's results.	High	Low	Medium	Confidentiality Privacy Availability
8	Security	Data protection. <i>Description:</i> The risk of doctor sharing suspicions of malignancy based on results with another person without the patient's approval.	High	High	High	Privacy Confidentiality
9	Security	Intercepting data in transit. <i>Description:</i> The risk of disclosure from a doctor or nurse when processing the referral form between different places, computers or sites.	High	Medium	Medium	Availability Confidentiality

Table 7-3 Updated Risk Register with Security Goals

7.4.6 Identify Countermeasure

After evaluating the risk level and security goals, the countermeasure symbols identified in Secure*BPMN (Cherdantseva, 2014) were adopted to indicate the appropriate countermeasure for each risk in the process model. Information Security Management Systems (ISO 27000) and Information Security Management in Health (ISO 27799:2008 and 2016) were used to specify the details of the countermeasure in the risk register. For instance, for the activity, the Dr. diagnoses a patient, the risk of safeguarding the patient's information requires a technical countermeasure as the doctor must have the right authentication and authorisation based on his role in storing medical health records and safeguarding the with the main security regulations. Figure 7-5 presents a BPM diagram for part of the GP Referral in Doctor Process with all countermeasure symbols for all risks. Appendix E.2 shows the full diagram and Appendix E.3 presents a full table for the GP Referral process.

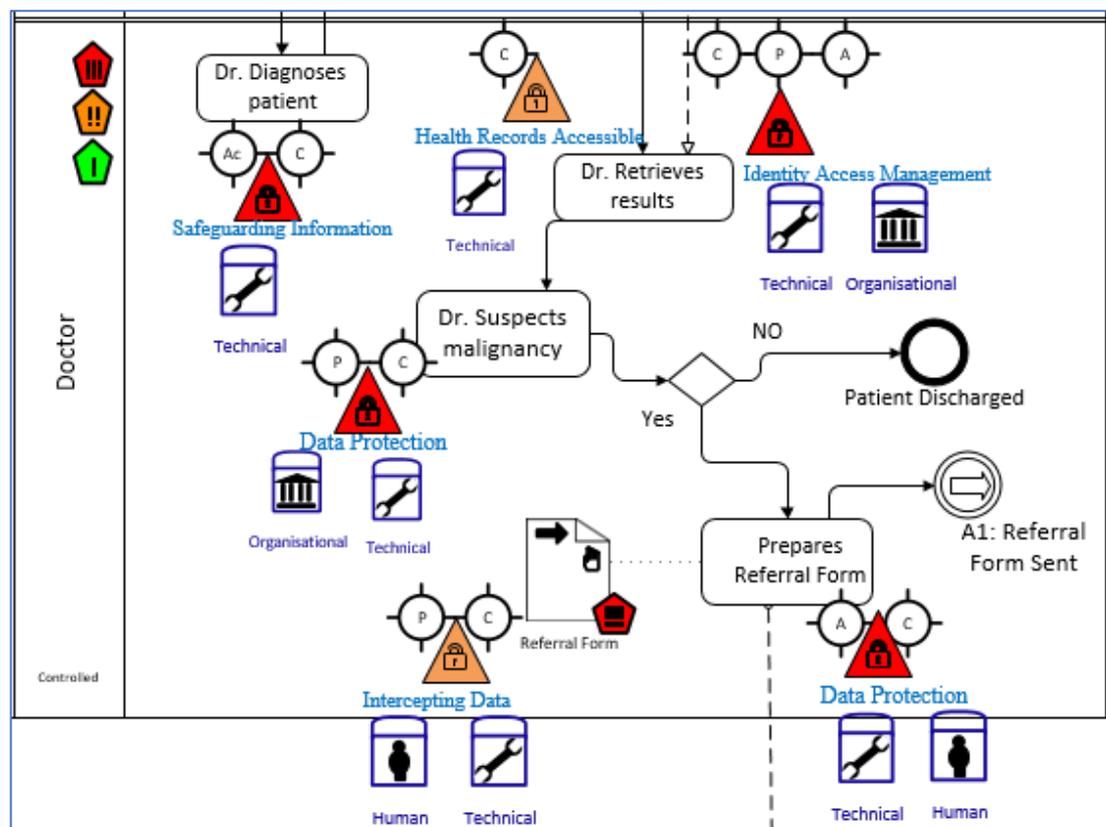


Figure 7-5 Countermeasure Security Risks Identified in Doctor Process

7.4.7 Updated Risk Register Table with Traceability

The Risk Register table was used as an input at this stage to add a traceability column (Table 7-4) which is not usually listed in the ordinary risk register table. It is important to trace the risk by showing its location and activity process which occur within it. Appendix [E.3](#) presents a Risk Register Table for GP Referral, Appendix [E.5](#) Risk Register for Hospital 1, Appendix [E.7](#) Risk Register for Hospital 2 and Appendix [E.9](#) Risk Register for Hospital 3.

No	Risk Type	Risk Name	Impact	Likelihood	Risk Level	Security Goals	Risk Countermeasure	Traceability
5	Security	<p>Safeguarding the patient's confidential information and compliance.</p> <p><i>Description:</i> Risk of doctor disclosure of the patient's confidential information to someone else from the diagnosing process.</p>	Very High	Medium	High	Confidentiality Accountability	<p>Technical: Doctor must have the right authentication and authorisation based on his role in storing medical health records and safeguarding these with key security regulations.</p>	<p>Process: GP Referral</p> <p>Location: GP Surgery</p> <p>Activity: Doctor diagnoses the patient</p>
6	Security	<p>Health records accessible.</p> <p><i>Description:</i> The risk of doctor retrieving the results of another patient from medical records.</p>	Very High	Medium	High	Confidentiality Privacy Availability	<p>Technical: Doctor needs the authorisation to access and retrieve the results of a patient within his team of care as well as supporting privacy guidelines.</p>	<p>Process: GP Referral</p> <p>Location: GP Surgery</p> <p>Activity: Doctor retrieves patient results</p>

Table 7-4 Sample GP Referral- Doctor Process Risk Register Table

7.5 Evaluation Methodology

To evaluate the MSR-BPM, the MSR-BPM approach was presented to Dr Cherdantseva. She provided positive feedback and stressed that this method would help in structuring and organising risk-related information. Also, she approved the expansion of the RMIAS and Secure*BPMN (Cherdantseva, 2014) by adding risk management to it. In fact, expanding the RMIAS to capture risk assessment was stated as an area for future work.

This research approach focused on using the BPM to model risk and enhance it with a risk register document by following Information Security Risk Management (ISO 27005) key processes, as shown in [Figure 7-6](#). Therefore, the main activities in Risk Management Process were focused on evaluating the MSR-BPM approach. Focusing on the risk management policy, five leading questions were identified :

- Who: is required to report, communicate, and take action?
- What: is required to be reported by staff, managers, executives, governance and committees?
- When: are risks to be reported and when is information to be disseminated to the clinicians, staff, executive and management committees/governing body?
- Where: is information stored, and communicated?
- How: are tools and processes to be used – e.g. risk assessments, risk registers, BPM?
- When: may a risk be removed from the current risk register?

These questions were employed in the comparison table between Risk Register and Business Process Modelling (BPM) in [Table 5-12](#) in Chapter 5, based on the key processes of the ISO 27005 to enhance the importance of combining both elements in managing security risks.

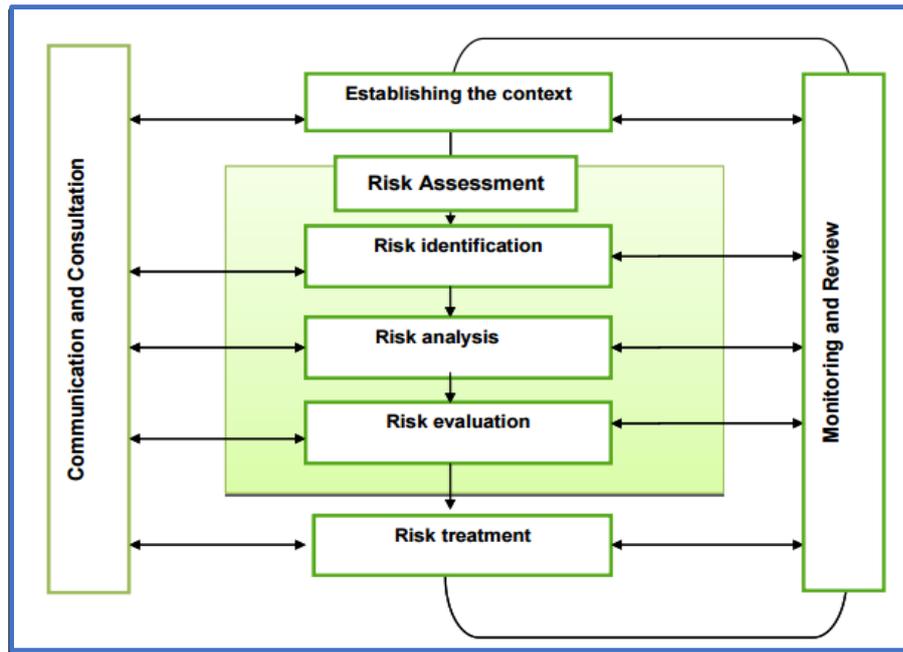


Figure 7-6 ISO27005 Information Security Risk Management Process

Information Security Risk Management (ISO 27005) processes were used to structure the evaluation which will be discussed in the next section.

7.6 Evaluation Methodology for MSR-BPM

Based on the comparison table between risk register and business process modelling in Chapter 5, the literature was reviewed in terms of quality criteria that are essential to fulfil in a system requirement. The SQuaRE Standard (ISO 25010) is widely used as a software product quality criteria which helps in identifying a broader range of quality aspects. The evaluation was influenced by the SQuaRE criteria to evaluate the work. In addition, the review of the literature explored evaluation methods for other approaches, such as the Method Evaluation Model (MEM) (Moody, 2003) to evaluate Secure*BPMN. Figure 7-7 elucidates the BPM for the evaluation methodology for the MSR-BPM approach.

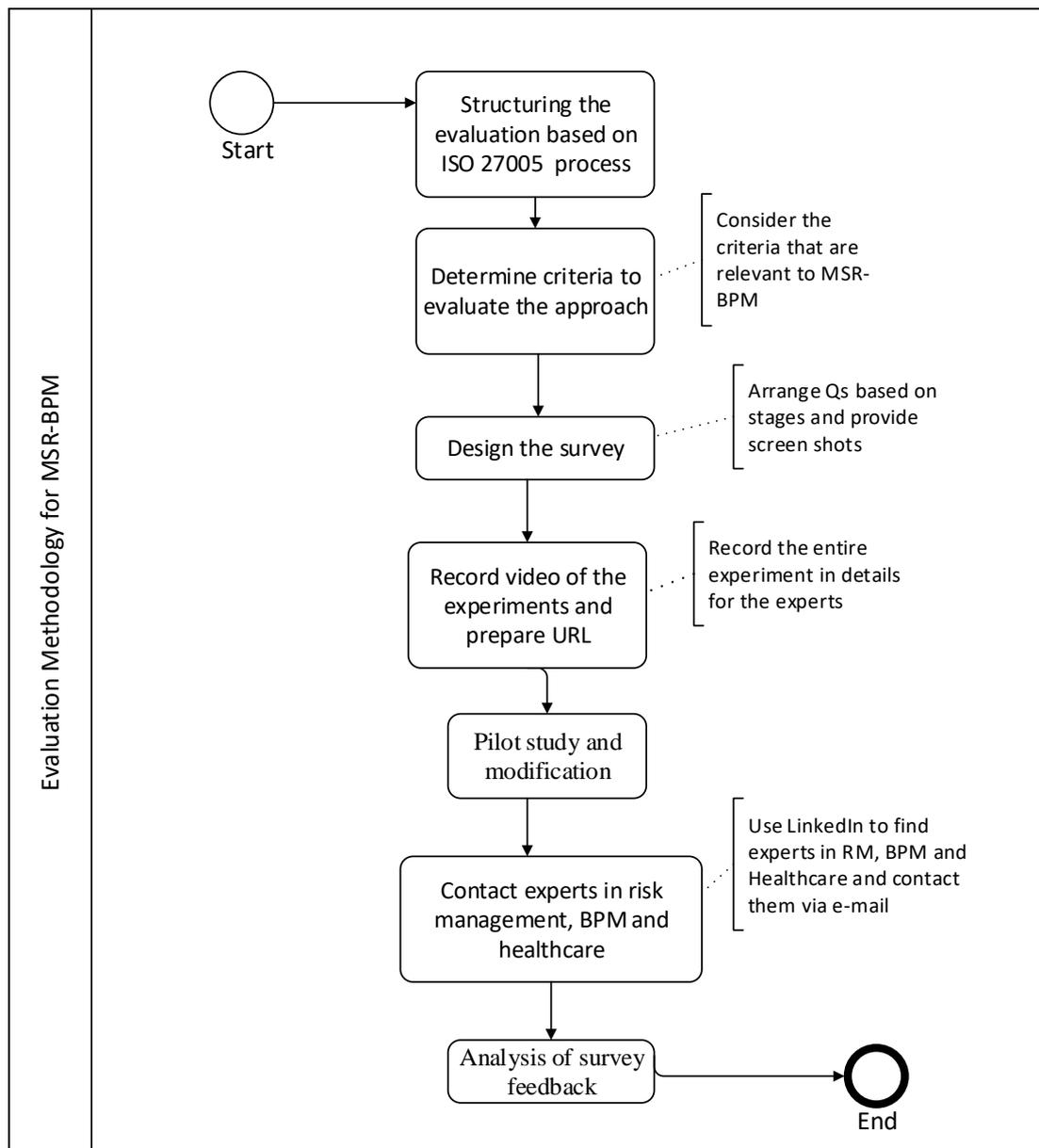


Figure 7-7 BPM of Evaluation Methodology

7.6.1 ISO 27005 Risk Management Processes

Questions were designed for all stages to enhance using the risk register to document risk assessment and countermeasures with business process modelling. Both methods complement each other by visualising the complex process and providing detailed analysis of the countermeasure needed for each risk.

7.6.2 Design of the Survey Questions

The survey started with a brief introduction about the researcher. The main purpose of performing the experiment which was assessing an approach for security risks in the healthcare domain that combines Business Process Modelling with Risk Register was also stated. The targeted practitioner/researcher was in Risk Management, Business Process Modelling and/or healthcare. Also, the survey explained that the evaluation process would be through watching a video (approximately 11 minutes) then answering questions to evaluate the proposed approach. The video outlined the healthcare scenario and demonstrated how the approach could be applied to manage security risks associated with the scenario. The video covered a subset of the scenario's processes and activities so a full set of process models with their associated Risk Register were provided for reference (Appendix [E.1](#)). A sample of the letter sent out is available in Appendix [F.1](#). In Questions 1 to Question 13, the participants were asked about their role in an organisation, as shown in Appendix [F.2](#). They were asked about risk management methods, and the nature of their experience, whether from research, practice or both. Also, they were asked about their Business Process Modelling experience over a number of years, the nature of their experience as well as the BPM methods they were familiar with. In addition, they were asked about their experience in healthcare.

The survey was anonymous, and no personal details were collected from the participants. They were questioned about their level of expertise in risk management, BPM and healthcare. Each response was based on a 4-point Likert scale:

Expert Competent Some knowledge No knowledge.

According to Joshi et al. (2015), the 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.

Also, based on SQuaRE quality criteria, survey questions were designed and compiled to validate MSR-BPM for all stages. The main aim of the evaluation was to ensure

that the MSR-BPM approach complied with the formal requirements of a well-established framework that is widely used for the assessment of the quality of modelling languages. Appendix F.2 presents the full set of survey questions. Figure 7-8 presents an example of the survey questions layout.

Stage 3: Risk Analysis and Evaluation

No	Risk Type	Risk Name	Impact	Likelihood	Risk Level	Security Goals
5	Security-1	<p>Safeguarding patient confidential information and compliance</p> <p>Description: The risk of Nurse disclosure patient results to someone else without the right approval during the preliminary tests conducted</p>	Very High	Medium	High	Confidentiality Accountability

Q18: Using both the process model and risk register approach helps staff to clearly identify the appropriate security goals and risk level with each risk.

Strongly Agree
 Agree
 Neither agree/disagree
 Disagree
 Strongly Disagree
 I do not know

Q19: The Risk Register-BPM approach used is more likely to be effective in the analyses and evaluation of risk than using a risk register only.

Strongly Agree
 Agree
 Neither agree/disagree
 Disagree
 Strongly Disagree
 I do not know

Figure 7-8 Sample of the Survey Questions Design

Questions 14 to 25 were based on the ISO27005 and main processes. The answer to each question was measured using a 7-point Likert scale:

Strongly Agree | Agree | Neither Agree/Disagree | Disagree | Strongly Disagree | I do not know.

During the literature review of quality evaluation (Moody, 2003), a number of quality standards (e.g SQuaRE ISO 25010) were reviewed to determine a set criterion to evaluate the MSR-BPM approach. It was necessary to ensure the right quality criteria was involved in the evaluation of the approach to determine the effectiveness of the proposed MSR-BPM approach in enhancing the communication of information security risk in healthcare processes.

The SQuaRE Standard (ISO 25010) is widely used in identifying a broad range of quality aspects. An appropriate criterion such as effectively applied, effective communication, useful and clear understanding was adopted based on the MSR-BPM context. The term ‘effectiveness’ is defined as “*accuracy and completeness with which users achieve specified goals*” (ISO 25010, 2011). The questions statement in Q14, Q19, Q20 and Q24 are used to measure effectiveness.

The term ‘usefulness’ is defined as the “*degree to which a user is satisfied with their perceived achievement of pragmatic goals, including the results of use and the consequences of use*” (ISO 25010,2011). The questions statement in Q15 is used to measure usefulness.

Also, the term ‘usability’ is used and defined as the “*degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use*” (ISO 25010,2011). The questions statement in Q16, Q17, Q18, Q21, Q22, Q23 and Q25 are used to measure usability.

Using ISO 27005 processes;

- At stage 1, participants were asked whether using the BPM effectively applied within the healthcare domain and if it was useful in establishing the context for stage one.
- At stage two, they were asked if the BPM could identify security risks and the likelihood of security risks associated with the roles.
- At stage three for risk analysis and evaluation, participants were asked about how effective the processes were to identify the security goals and risk evaluation.
- At stage four for risk treatment, they were asked if the MSR-BPM effectively helped in identifying the appropriate countermeasure.
- At stage five for monitoring and reviewing, the main concern was knowing if the MSR-BPM could identify change with risk position and whether it was in process, activity or inflow.
- At six stage of communication and consultation, it was necessary to ascertain whether the MSR-BPM approach was clearly understandable and appropriate to manage risk, effective communication and provide a shared understanding of risks as well as managing risks in compliance with the ISO 27005 processes.

Table 7-5 presents a justification for questions 14 to Q25 to evaluate MSR-BPM approach.

ISO 27005 Stages	Question No.	Question	Justification
Stage 1	Q14	The BPM approach used can be effectively applied to capture processes in healthcare.	To know if using BPM is effectively applied within the healthcare domain.
	Q15	The BPM approach used is useful for designing process models as it helps to clearly identify activities, flows, locations and roles in healthcare processes.	To know whether MSR-BPM is useful.
Stage 2	Q16	The BPM approach used can clearly identify security risks with different activity levels in healthcare processes.	Clear identification of security risks.
	Q17	The BPM approach used is more likely to help staff identify the appropriate security risks associated with the roles compared to relying on a Risk Register only.	To identify the likelihood of occurring and security risks associated with the roles.
Stage 3	Q18	Using both the process model and risk register approach helps staff to clearly identify the appropriate security goals and risk level with each risk.	Identify security goals and risk level.
	Q19	The Risk Register-BPM approach used is more likely to be effective in the analyses and evaluation of risk than using a Risk Register only.	Effective analysis and evaluation of risk.
Stage 4	Q20	The Risk Management-BPM approach used is more likely to be effective in identifying suitable countermeasures in the healthcare domain than using risk register only.	Effective in identifying countermeasure.
	Q21	Using Risk Register and BPM together is more likely to help in identifying the appropriate countermeasure.	To identify the appropriate countermeasure.
Stage 5	Q22	Using Risk Register and BPM together is more likely to help in identifying any changes with the risk than using risk register only.	Identify change with risk.

Stage 6	Q23	The Risk Register–BPM approach used is clearly understandable and appropriate to use to manage security risk in healthcare processes.	To know if the MSR-BPM is clearly understandable and appropriate to manage risk.
	Q24	Risk Register-BPM approach used is more likely to effectively communicate risks to achieve a shared understanding of all roles involved in the process compared to using Risk Register only.	Effective communication and providing shared understanding of risk.
	Q25	Developing BPM and risk register for key health processes is more likely to help healthcare organisations manage security risks in compliance with Information security risk management practices (ISO27005) compared to developing a Risk Register only.	To know if MSR-BPM manages risk in compliance to ISO27005

Table 7-5 Justification of Survey Questions to Evaluate MSR-BPM Approach

7.6.3 Pilot Study of the Experiment

A pilot test of the experiment was performed with two academics. The approach to the experiment was initially refined in response to the feedback received from the thesis’s supervisor, Dr. Wendy Ivins. Also, it was sent to Dr. Yulia Cherdantseva in order to test the logical flow of it; the BPM diagram was clear and the explanation for each stage was obvious and explicit. The video and survey were refined according to the feedback received in the pilot test; the clarity of the experiment material was improved, as a result. Then, the evaluation material was sent via e-mail to all the participants who agreed to participate in the evaluation experiment. The material of the evaluation includes a URL of the video, Survey Questions and a Full set of BPM and Risk Register for the healthcare scenario. See [Appendix E](#).

The evaluation was not performed in Oman as it was not possible to find sufficient experts in risk management, business process modelling or healthcare.

7.6.4 Record Video of the Experiments and Prepare URL

The complete set of the evaluation scenario of the Integrated Care pathway for Breast Cancer treatment was recorded by providing the actual scenario, BPM for all stages, BPM for identified risks, BPM for risk evaluation, security goals and risk countermeasures. In addition, the video shows the output of how the risk register will look and provides an electronic document of all the deliverables (Appendix [E](#)).

7.6.5 Contact the Experts

Networks established by the School of Computer Science and Informatics were used to contact the experts in risk management, business process and health care to evaluate the MSR-BPM approach. A sample of the letter sent out is available in Appendix [F.1](#). The evaluation experiment process consists of three main parts:

1. Watching a video that is approximately 11 minutes long through the URL: <https://youtu.be/R0idfl9McJE>. The video outlines the healthcare scenario and demonstrates how our approach can be applied to manage security risks associated with the scenario. The video covers a subset of the scenario's processes and activities, so a full set of process models with their associated Risk Registers in Appendix [E](#) was provided for reference.
2. Answering questions to evaluate the MSR-BPM approach proposed for Security Risk Analysis and Business Process Model according to the ISO 27005 activities.
3. Post-task survey, the participants were asked to provide their opinion regarding usefulness of the MSR-BPM.

The video is still available for anyone who would like an insight into the MSR-BPM approach.

7.6.6 Analysis of Survey Feedback

7.6.6.1 Participant Profile from UK

Twelve individuals participated in the empirical evaluation of the MSR-BPM from different areas of expertise in healthcare and security. They are experts in risk management (7) and business process modelling (6). Several of them are familiar with the healthcare industry (6). As Appendix [F3](#) and [F4](#) showed, the experience of the participants varies from 1 to more than 12 years. According to Chung and Nixon (1995), the qualitative IS research 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 Benbasat & Goldstein (1987) and Mayers & Newman (2007) respectively. The participants in this evaluation were asked to answer a survey questions based on a case study. Therefore, this research used qualitative methods to evaluate the MSR-BPM approach. All twelve participants came from the UK. A summary of the participants' profiles is provided in [Table 7-6](#). The full details are presented in Appendix [F.3](#) and [F.4](#) Table 1 and Table 2.

Risk Management			Business Process Modelling			Healthcare domain	
Expert	Competent	Some knowledge	Expert	Competent	Some knowledge	YES	NO
P2,P12	P1, P3,P7,P8,P11	P4,P5,P6,P9, P10	P3	P1,P2,P7 P11,P12	P4,P5,P6, P8, P9,P10	P2,P3,P7,P8, P10,P12	P1,P5, P6,P9, P11

Table 7-6 Summary of Evaluator Background.

7.6.6.2 Participant Feedback on Questions 14 to 25

The analysis was performed using Excel based on the survey stages to explore the participant perceptions and acceptance of using the MSR-PBM within the healthcare domain. [Figure 7-9](#) illustrates the findings for stage one. It can be seen that all

participants are in strong agreement in stage 1, which indicates strong acceptance for establishing the context and enhancing traceability. In particular, Q15 shows strong agreement regarding its effectiveness. Participants supported this by saying:

Participant 2: *“The value lies in improving traceability between the technology and the clinical setting.”*

Participant 4: *“Certainly more readable, understandable and referable than a potentially large and unwieldy risk register.”*

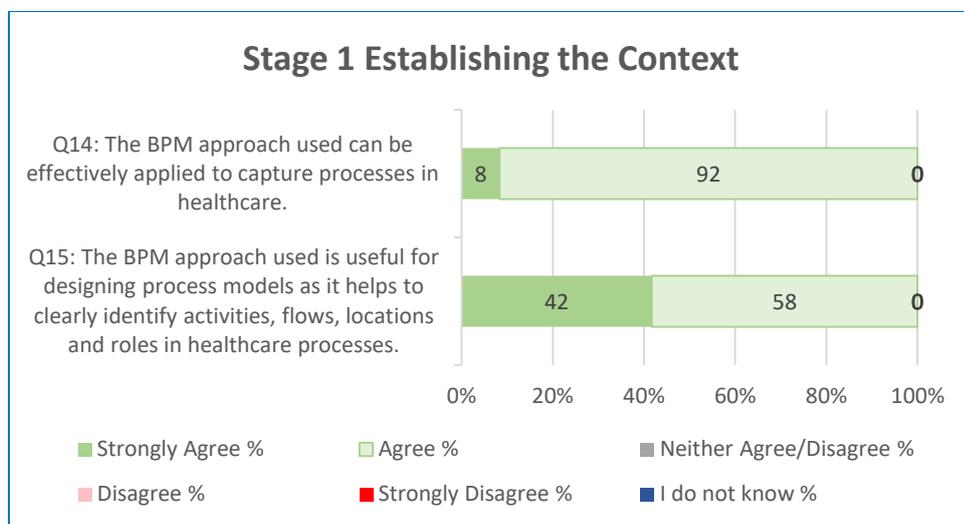


Figure 7-9 Summary of Stage 1 Analysis

On the other hand, in stage 2 (Figure 7-10), Identify Security Risks, Q17 indicates that the participants show some uncertainty that the MSR-BPM approach will help in identifying appropriate security risks.

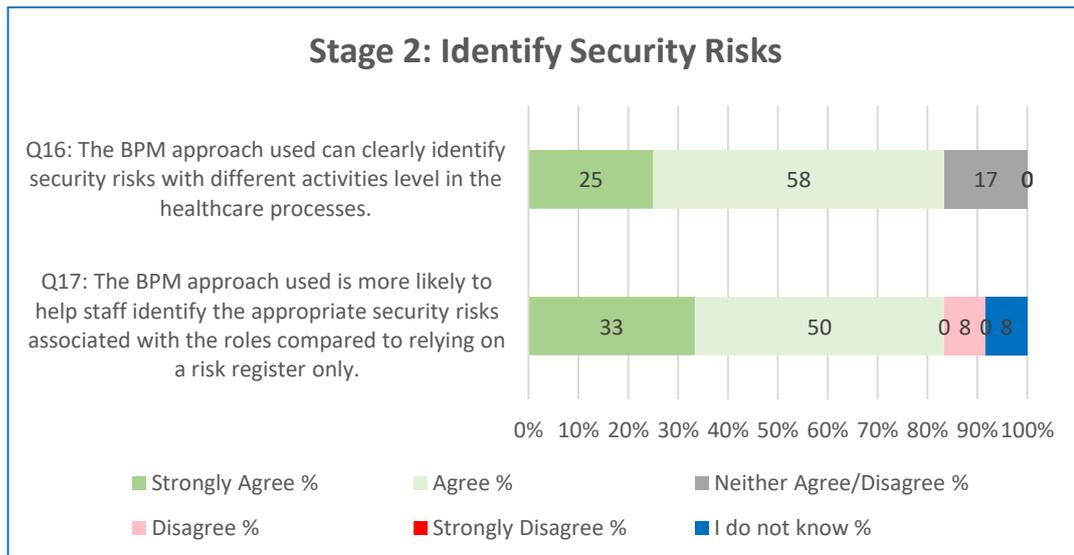


Figure 7-10 Summary of Stage 2 Analysis

Meanwhile, in stage 3 (Figure 7-11), Risk Analysis and Evaluation, Q18 and Q19 indicate the participants’ acceptance of using the BPM and risk register for risk assessment and evaluation. Participant 11 supported this by commenting, “I always find modelling to be very useful and I like the way that BPM is linked to the register”.

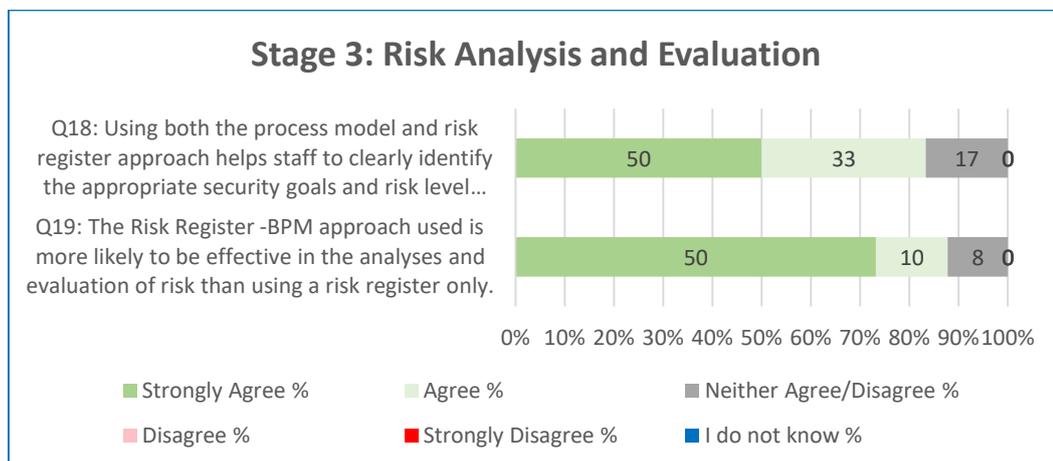


Figure 7-11 Summary of Stage 3 Analysis

Figure 7-12 presents stage 4; Q20 and Q21 demonstrate that the participants are not sure that this approach will be effective or helpful in identifying suitable and appropriate countermeasures. Participant 1 explains this as follows: “Regarding Q20 and Q21, I do not see how this method could actually help with identifying appropriated

countermeasures. They could be equally well identified based on the description of the problem provided in a risk register. It only depends on how detailed is the register and how detailed is a model. Although, I can clearly see the benefits of the method for structuring and organising risk related information, I am not sure that it assists with identifying countermeasures.”

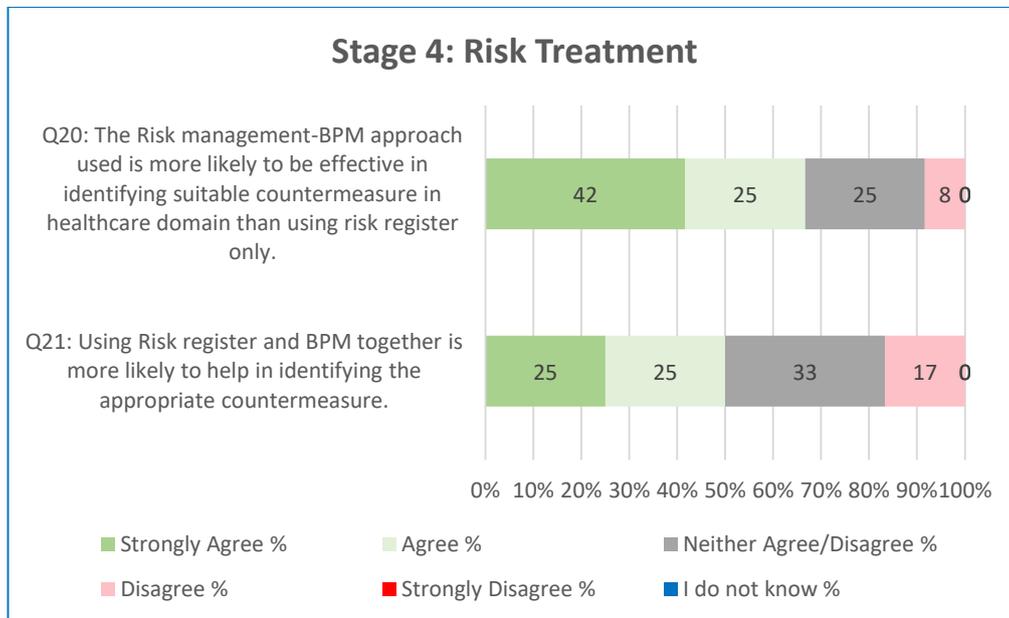


Figure 7-12 Summary of Stage 4 Analysis

In addition, in Q20, Participant 11 differentiated between the problem and solution and highlighted that the MSR-BPM can improve the understanding of risk but it does not offer a solution to the problem. Also, in Q21, Participant 11 emphasised that the statement was logical but it does not ensure that appropriate countermeasures will be implemented.

Participant 11: *“I think the solutions and problems are two different things. I think this approach is more likely to identify problem areas. What is done about them is (in my experience) far more likely to be affected by the security practitioners knowledge and other external factors such as available budget. The people implementing the countermeasures won’t be the people operating the BPM system in my experience. This approach will certainly provide better information about what the risks are but won’t guarantee that they will be treated”.*

Participant 11: *“But it will provide comprehensive information about the risk. The statement is logical but this doesn’t always guarantee that the most appropriate countermeasure will be deployed.”*

Stage 5 (Figure 7-13) represents a strong agreement that the MSR-BPM would help in identifying any changes within the risk rather than using risk register only. Participant 4 supported this as follows: *“Certainly more readable, understandable and referable than a potentially large and unwieldy risk register”*.

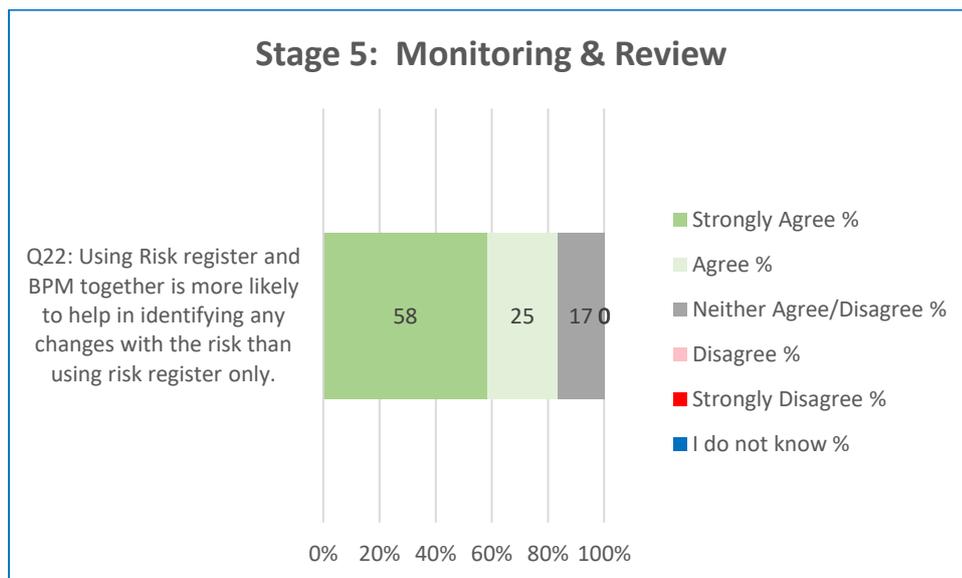


Figure 7-13 Summary of Stage 5 Analysis

Although stage 6 (Figure 7-14) shows strong acceptance for using the MSR-BPM as a tool to enhance communication and manage risks, it illustrates that some participants are not sure that it is clearly understandable.

Participant 3: *“It’s better than just a risk register but I haven’t seen it compared to CESGs approach to infosec risk management which as a public sector body they should adhere to”*.

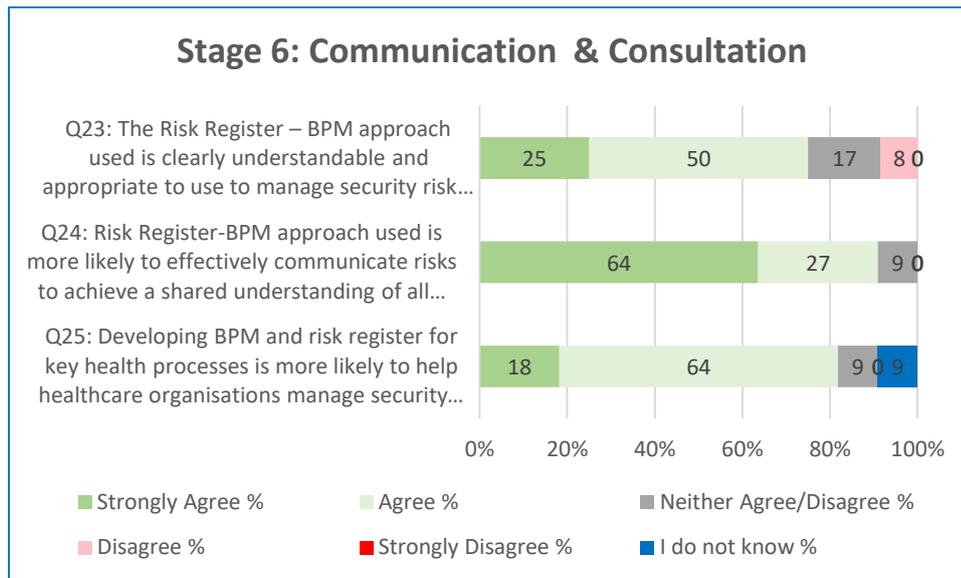


Figure 7-14 Summary of Stage 6 Analysis

7.6.6.3 Participant Feedback about MSR-BPM Q26 to Q29

In this section, open-questions were designed to allow for more feedback from the participants regarding the MSR-BPM approach.

Q26: Please outline any difficulties you may have experienced in following the Risk Register-BPM approach presented in the video.

Question 26 was created to understand whether there are any difficulties following the Risk Register-BPM approach. Most of the participants indicated that the method was easy to follow and no difficulties were mentioned, but they raised an important point that the user of the approach needed to be familiar with the area because a clinician or a nurse might not be aware of its modelling aspect. Also, the final output of the diagram looked overcrowded with all the annotations of access permissions from Secure*BPMN, risks, security goals and countermeasures. Hence, this aspect will be addressed in future research.

Participant 1: “I followed the method easily. My main concern is that the final annotated diagram is overcrowded with symbols which make reading and understanding harder. I would suggest that in future work you should consider how

to improve the effectiveness of the visual representation of annotated BPMN models.”

Participant 2: *“Who is the user of your approach? A security engineer or a clinician? I would say an engineer might be familiar with this sort of modelling. I doubt a clinician will have the skill or time to develop these models”.*

The MSR-BPM approach is very rich; what it represents in the BPM and what level of detail depends on the stakeholder’s team. The stakeholders’ discussions will allow team members to discuss each risk’s impact, likelihood and level rather than copying from previous risk register documents.

Participant 8: *“...People have a tendency to just copy by default what has gone before in the examples, as they stick with the defaults. Taking this into account for your examples would be quite helpful”.*

Participant 2: *“As a framework it’s fine. The problem is in having data/evidence to decide on things like likelihood and impact parameters”.*

Q27: Does the Risk Register-BPM approach used include any elements that are missing or not relevant to the Managing security risks domain? If yes, please name them.

In Question 27, the primary intention was to ascertain if there was any aspect missing or not relevant to managing security risks domain. Participant 1 placed emphasis on "Privacy" as an important element, especially in the healthcare field; this needs to be clearly considered and any issues pertaining to data anonymization needs to be addressed. In addition, 5 participants were considered to model other types of risks, such as physical access and data at rest. These types of technical risks are addressed in Reference Generic Table in [Appendix C](#).

Participant 1: *“Privacy is critical in healthcare, but at the same time data are collected for important medical analysis. So you may want, in future work, to consider representation or privacy and address issues of data anonymization”.*

To enhance the usefulness of the approach, it is important to capture customers' 'Feared Events' which would assist people in addressing the risks without thinking of the infrastructure, people, process and technology. Therefore, the approach will focus on the source of the risk and find a practical mitigation solution for it. Also, it is necessary to identify the *requirement* of the organisation or the customer to help in understanding various concerns or potential risks within their domain.

Participant 11: *“One of the things that we have found to be very useful is to take into consideration the customer ‘Feared Events’. These tend to be high level and help people to think about the risks without the constraints of current infrastructure / people / process / technology. It also helps in stopping people ‘solutionising’ (sorry – horrible word) too early in the process. This type of approach also helps people consider the risks introduced by process and people, as opposed to being purely technology focussed, which is a real problem in my experience. It is important for the security system design team to understand where the risks are derived from so that they can be effectively mitigated in the solution. Another useful question is to identify the organisations ‘crown jewels’ so that you know what is of most value to the customer. It is always useful to gain as many perspectives from as many different sources as practical. ”*

Q28: To what extent do you feel that Risk Register-BPM approach can be used as a valuable tool to complement using a risk register to manage security risks?

In question 28, the participants were asked if the Risk Register-BPM approach could be used as a tool to complement the risk register to manage security risks. They highlighted that the method could bring multiple benefits as it helps in visualising the entire process of security risks in the complex business process.

Participant 1: *“If used appropriately, the method could bring multiple benefits as it helps to visualise security risks in complex business processes, and make them explicit and easy to see for experts with different backgrounds.”*

Participant 7: *“To a great extent.”*

Participant 8: *“I think it is useful to have the visualisation for people so they can see the connections across an organisation and the flow. This is often what is missing a lot of the time”.*

Also, they considered it as more readable and understandable than the standard risk register document. They also believed that it might enhance traceability.

Participant 4: *“Certainly more readable, understandable and referable than a potentially large and unwieldy risk register.”*

Participant 3: *“It’s better than just a risk register but I haven’t seen it compared to CESGs approach to infosec risk management – which as a public sector body they should adhere to – hence harsh mark on Q23 – sorry –”.*

Participant 5: *“As I mentioned earlier, I quite liked the model and is a great starting point to evaluate risk particularly when establishing processes.”*

Participant 10: *“This model of three different hospitals may not be a universal model but it will be applicable in few scenarios. There would be some patient who will go from GP to Hospital 1 (usually holds the first and subsequent MDTs) for further assessment and then Hospital 2 for treatment (Hospital 2 will hold MDTs as well). But the scenario is a very practical one and associated risks are better identified using the BPM and risk register approach. Well done”.*

In addition, the MSR-BPM is more like a living document than the commonly used risk register, which tends to be ignored after the initial project is implemented.

Participant 11: *“I think it would be an improvement on what currently exists. We are often presented with a risk register during consult / system design phases which tend to be a cut and paste of the last one with no real thought into the actual risk. It would be more likely to be a living document than a risk register which tend to ignored after the initial project implementation.”*

Providing a training session for using the MSR-BPM is important as some of the participants raised concerns regarding the use of the MSR-BPM by non-technical stakeholders.

Participant 6: *“Have the right methodology and tooling is essential for managing security risk. Having a methodology that is sound is good, and I think this can be used, but you would need to spend the time not just creating the method but also building the training and implementation capability, as people performing this work are incredibly busy and don’t always have time to learn new methods if the methods they are using are ‘good enough’ Being a better method is not always a good enough reason to stop doing what has been working, so you’ll need to construct a compelling reason not just why this is good, but also why the current method is not good.”*

The MSR-BPM has a substantial importance in terms of understanding the risk holistically compared to a traditional risk register. Therefore, the MSR-BPM is a helpful tool in identifying risks through a logical process flow.

Participant 9: *“I feel it is of significant value in comparison to a traditional risk register. If this was applied in detail to a very specific hospital / health care facility, it could be used as starting point to understand risk, referencing out to more detailed documents to form a holistic risk analysis. If this were updated as departmental processes evolve, it could be used to inform the ‘plan’ aspect of a health care providers ISMS.”*

Participant 10: *“It is useful in explaining the underlying process and in my opinion stakeholders will find it helpful to view the exact points/processes which have underlying risks.”*

Participant 12: *“It will be a helpful tool in identifying some risks through a logical process flow, however it shouldn’t be used in isolation. Equally, risk registers are used for simplicity and the ability of a wide audience to be able to consume their outputs and contribute. It’s possible that whilst this is good for a technical audience, you may have security risks that threaten brand or more nebulous economic value. It’s likely stakeholders you’d want to engage in this process won’t be from a technical background and may struggle conceptually with it, so alternative techniques may be required.”*

Q 29: Do you anticipate any problems with adopting the risk register-BPM approach? If yes, please outline them in in detail here.

In Question 29, the participants were asked if they anticipated any problems with adopting the risk register-BPM approach. Some participants argued that the MSR-BPM is not a standard and therefore it would require extensive testing and several rounds of evaluation for improvement before being implemented in practice. Others consider the user acceptance as a critical issue, especially if the user does not have a technical background. Therefore, having stakeholder teams from multidisciplinary fields would help in this aspect.

Participant 1: *“As this is not a standardised or widely used method, I anticipate a lot of difficulties with adopting a method in large and heavily regulated organisations. The method would have to go through a lot of empirical testing, and several rounds of evaluation and improvement before it may be adopted in practice”.*

Participant 2: *“User acceptance might be an issue, especially if the intended user is not an engineer, e.g. doctor or nurse.”*

Participant 3: *“would be fine but as part of a wider RMADS / approach to implementing GPMS – basically needs lots of scoping documents and quite a lot of other stuff – after recent events this is likely to be pretty important.”*

Participant 4: *“It would depend on how process varies across hospital ‘constituencies’ in the UK – is the process totally standardised across all hospitals? (I don’t know the answer to that)”.*

On the other hand, some participants argue that most organisations already have a risk template that they follow. Therefore, they will not likely be receptive to a different method. Having a Multidisciplinary stakeholder team could encourage them to embrace the approach as it will enhance people’s understanding of risk impacts, regardless of diversity of experience.

Participant 5: *“The only problem I can think of is that most organisations already have a risk template that they follow with different level schema, which could involve*

a lot of levels (A1,A3, B3, etc.) and it might be difficult to map their existing schema with the three levels (Red, Amber and Green)”.

Participant 6: *“What I mentioned above. It’s hard in busy spaces, especially in health care, to learn and use new things. This would have to be used by multiple practitioners in different hospitals for it to be effective, with the underlying DB constructed in a way to collect the right information, so to make this effective it’s not just convincing one manager or one hospital, but a group of them working together. Is there a need for this in the marketplace? Do hospitals see a problem with what they are using to demand something better? ”*

In addition, some participants had concerns about people’s capacity and time needed to carry out the MSR-BPM method as people are busy and do not have time to learn and adopt new methods. This research carefully considered the need for training and awareness sessions as a necessary activity for all staff to enhance the importance of identifying risk within the whole process.

Participant 8: *“As mentioned above I would question the time and capacity people have to do this. They are often stretched for time, why would they adopt this over just keeping with the risk register? As much as it’s known risk registers aren’t the best and have many issues, how will you bring people with you, to make them understand what could be done with this work?”*

Participant 11: *“The supporting functions such as training and system management of implementing such a system at scale should not be under estimated. Systemic change is always difficult. Typically, the change management function within the organisation would look after the living document so system change in that area would be required.”*

Q30: Any other comments or feedback?

One participant did not answer the questions as they found it difficult.

Participant 2: *“It was hard to answer your questions since you do not provide a reference/benchmark against which to compare your approach. For example, is it nothing vs your approach? Or using flowchart vs BPMN? This makes a big difference”.*

As a suggestion for effectiveness improvement, Participant 11 recommends linking the MSR-BPM with the security systems. This can be earmarked for future research as it will help in measuring the countermeasure effectiveness to mitigate the identified risks or not.

Participant 11: “... *To be effective it would also need to be linked to the security system design documentation to measure how well the identified risks are mitigated (or not) as the systems capability (in terms of people, process and technology) change over time.*”

7.6.6.4 Evaluating MSR-BPM with Stakeholder from Oman

The researcher liaised with practitioners from Oman to evaluate the MSR-BPM approach. Verbal communication was conducted with practitioners from the healthcare and Information Technology Authority. A confirmation assured their willingness to participate. The evaluation material, which included a formal request letter to explain the research aims and objectives, the experiment’s URL, deliverable output and survey questions, were sent via e-mail on 23rd May 2018. A kind reminder was sent on a weekly basis. Unfortunately, there was a lack of response to emails. Only one respondent replied via email out of twenty.

From the feedback received, it was revealed that the practitioner faced difficulty in following up the experiment video as she was not familiar with the terminology of risk register and BPM. She commented, “*I’m terribly sorry my dear for not being able to help you with the survey. The difficulty was in that I found the video too long but of course I understand that you needed the time to explain the topic. The second difficulty was the technical terminology which I had a problem to cope with, I’m not sure if anything needs to be changed because maybe someone else will be in a better position than me to understand the concept and fill the survey*”.

In addition, she indicated that the risk register was not in use in their workplace. However, an electronic incident reporting system where they enter their medication errors and any incidents which may be technical or environmental was in use. She maintained that the system also incorporated error types and causes which are entered through drop down lists and free text format. The system then produces reports when needed.

The researcher tried to request further responses and other evidence of using risk register within the healthcare in Oman. However, it was not possible to find any evidence that risk register is adopted in the healthcare in Oman. This may explain the lack of responses from practitioners in Oman as they are unfamiliar with the technique used in this methodology.

The lack of adoption of Risk Registers in the healthcare in Oman would be a barrier to migrating the MSR-BPM approach in the Omani context. However, the MSR-BPM is suitable for any organisation that is familiar with the ISO 27000 standards and could also be adopted by organisations that are familiar with the ISO 31000 standards.

The Omani healthcare system has not yet adopted the concept of patient pathways. According to World Health Organization (WHO, 2017) Oman has extensive plans to strategically implement initiatives to make health care systems “patient-centred”, i.e. a system that provides care that is “respectful of and responsive to individual patient preferences, needs and values, and ensuring that patient values guide all clinical decisions” (WHO, 2017). If Oman moves to patient-centred system, MSR-BPM approach will help in providing shared understanding of anticipated risks within patient pathways.

7.6.7 Evaluate MSR-BPM in ISO 27005 Process

7.6.7.1 Advantages of MSR-BPM

It was decided to reflect on the MSR-BPM approach based on the ISO 27005 process (Figure 7-6) to show its effectiveness and the extent to which it satisfied all process requirements. The anticipated benefits of combining risk register with BPM (in section 5.4, Table 5-12) form the roadmap for the reflection. The MSR-BPM helped in establishing the context by identifying the scope and boundaries of the context that needed to be reported by creating the BPM. The MSR-BPM diagram shows who is required to report and communicate risks within an organisation. Also, the MSR-BPM approach is highly effective in helping staff understand what the risks associated within their roles are. Participants are in strong agreement regarding the MSR-BPM, as shown in the analysis section 7.6.6.2 for stages 1, 2 and 3. In addition, Participants 8 and 10 provide positive comments in terms of visualising the risks within a process.

Participant 8: *“I think it is useful to have the visualisation for people so they can see the connections across an organisation and the flow. This is often what is missing a lot of the time”.*

Participant 10: *“It is useful in explaining the underlying process and in my opinion stakeholders will find it helpful to view the exact points/processes which have underlying risks. The scenario is a very practical one and associated risks are better identified using the BPM and risk register approach. Well done”.*

The MSR-BPM is vital in terms of understanding the risk holistically compared to the traditional risk register. It is a helpful tool in identifying risks through a logical process flow. Another advantage can be seen in the way it allows structuring and organising risk-related information. The MSR-BPM is useful in risk assessment (risk identification, risk analysis and risk evaluation) as it determines the risk name and type with a brief description in the risk register. It also provides information on the impact, likelihood and risk level.

Participant 4: *“Certainly more readable, understandable and referable than a potentially large and unwieldy risk register”.*

Participant 5: *“...I quite liked the model and is a great starting point to evaluate risk particularly when establishing processes.”*

Participant 9: *“I feel it is of significant value in comparison to a traditional risk register. If this was applied in detail to a very specific hospital / health care facility, it could be used as starting point to understand risk, referencing out to more detailed documents to form a holistic risk analysis. If this were updated as departmental processes evolve, it could be used to inform the ‘plan’ aspect of a health care providers ISMS.”*

Participant 12: *“It will be a helpful tool in identifying some risks through a logical process flow.”*

The MSR-BPM approach improves the communication mechanism between different rows and locations by providing all parties with a shared understanding of the risks as they are tested through the application, as explored in Chapter 5 in section 5.3 for the hypothetical case study. In addition, it enhances traceability of risk changes. Therefore, the MSR-BPM approach helps in the Monitoring and Review process by identifying any changes within a risk rather than using the risk register only. The BPM diagram will update the process to clearly visualise the risk changes, whether at the process or activity level.

Participant 11 supported this by commenting, *“I always find modelling to be very useful and I like the way that the BPM is linked to the register. I think it would be an improvement on what currently exists. We are often presented with a risk register during consult / system design phases which tend to be a cut and paste of the last one with no real thought into the actual risk. It would be more likely to be a living document than a risk register which tend to ignored after the initial project implementation.”*

Although the findings from the interviews and questionnaire in Chapter 3 address other types of risks, such as Management, Technical, Legal and other Risks not specific to cloud computing (listed in [Appendix C](#)), the time constraints of the research made it difficult to address all risks in detail. Therefore, the primary focus of this research was centred on security risks. Besides, there were risks that had dependencies on other risk categories, that may affect or increase the current risks or create additional risks. For example, lowering the labour number can reduce cost but can also create a stressful environment for other labour, which may lead to a reduced quality of work.

This research emphasises the importance of combining Risk Register with BPM because the major limitation of BPM is that it does not provide in-depth details about countermeasures. Hence, having the risk register table helps to document countermeasures in more depth.

7.6.7.2 Limitations

Applying Information Security Management Systems (ISO 27000) in the healthcare domain is a challenge because it involves high level guidelines. In addition, the time available to study the ISO 31000, ISO 27001, ISO 27002, ISO 27799:2008, ISO 27799:2016 and ISO 19510 was limited. The researcher had limited experience with both systems design and the healthcare domain; therefore, one of the MSR-BPM limitations was that it took time to draw the BPM diagram. Also, it was a challenge to know the level of details required to be included in the BPM diagram. Some might argue that the countermeasures can be removed from the BPM, but there is a need to structure thinking and visualise the risks for stakeholders. Others may suggest removing the level of access abstraction from the BPM to make the final annotated diagram less crowded with symbols and as a result reading and understanding becomes more user-friendly. The stakeholder team decides the level of detail required in the diagram according to the situation they are dealing with. Therefore, it helps to have an experienced business analysts as part of the team.

A reflective practitioner commented that it is a challenge to draw complex scenarios and therefore a Multidisciplinary team is required to work on the MSR-BPM approach to discuss the right level of abstraction and to determine the risk level. Also, deciding the countermeasure for each risk is not an easy task as some risks are applicable to more than one countermeasure.

The MSR-BPM is not a standard or commonly used method; therefore, user acceptance might be another obstacle as people might not accept new methods easily. Thus, several rounds of evaluation and improvements would be necessary before adopting the approach in practice.

The experts/practitioners were right in that the limitation of MSR-BPM is that it is not effective in risk treatment because it does not help to determine the appropriate countermeasure to mitigate the risk. It does help document the countermeasure once it is identified by the stakeholder, however. Hence, there is a need for a Multidisciplinary team to assist in suggesting the risk mitigation countermeasure based on their knowledge and expertise.

7.6.7.3 Evaluation of the Approach to Determine Risks

The literature review helped to identify various types of risks in using cloud computing in healthcare services. A range of risks were identified covering management, technical, legal and security risks. However, many of the risks were either high-level or too specific to a particular context. 18 risks from the literature review were developed into a risk register in Chapter 2 (Table-2-3). The risk register was enhanced with an analysis of importance and relevance to the healthcare context in Oman. It also incorporates some of the operational risks associated with central cloud infrastructure managed by the ODP and ITA-Cloud. However, developing a risk register through a survey of the literature alone gave an insufficient coverage of the risks and the sources did not always provide appropriate countermeasures for mitigating the risks. Further

an analysis was needed to understand the stakeholders' perceptions of using cloud computing services within healthcare in Oman.

The high-level risks in [Table-2-3](#) were useful to build up the questionnaires in Chapter 3 as it focussed on Management, Technical, Legal and Security Risks. Each area was expanded further according to surveys adopted from literature (Lian et al., (2014); Wijaya et al., (2014); Singh et al., (2014) and Chang et al., (2007)). The main finding of the questionnaires centred on identifying security and technical risks as main concerns. This was also confirmed in an interview with H.Dr. Ali Talib Al Hinai, Undersecretary for Planning Affairs in Ministry of Health who highlighted the need for an effective security risk assessment methodology to overcome the identified security concerns. Thus, the scope of the risk analysis was narrowed to the technical and security aspects of cloud computing.

A framework was used to help identify and manage risks. The RMIAS (Cherdantseva, 2014) was chosen because it provides the most comprehensive set of security aspects. It provides an analysis and classification of security aspects proposed by reference models on information assurance and security. Also, it is based on Information Security and Information Assurance standards and the ISO/IEC 27000 family of standards. However, RMIAS did not cover risk management in detail but the model was adapted, so that the Security Development Life Cycle Dimension (the top left quadrant) was replaced with the Information Security Management System (ISMS) process from the ISO 27005 so that Risk Management became the primary focus. This was used to develop a generic risk register table to document the risk name and risk description. The structure of the risk register was used to determine the taxonomy of risk information, such as risk identification, risk analysis and risk evaluation. An ordinary risk register table does not have a security goal, but it is important to identify suitable countermeasure needed.

The European Union Agency for Network and Information Security (ENISA) was used as a guideline to identify the impact, likelihood and risk level for each risk because it holds security risks, technical risks and other types of cloud computing risks. A mapping process between the survey statement which identified the technical and security aspects and ENISA guidelines list of risks was performed. The mapping process resulted in creating a generic reference risk register table which holds 46 risks ([Appendix C](#)) rather than 18 risks which were identified in the literature (Chapter 2 [Table-2-3](#)).

The 46 risks were a mixture of areas related to different risks management perspectives. They include: Change project risks associated with introducing cloud computing into the hospitals, Operational risk associated with central cloud infrastructure managed by ODP and ITA-Cloud and Operational risks within each hospital.

Despite risk register benefits (section4.9), there are limitations in using the Risk Register alone as it lacks risk visibility within a process. Thus, the methodology was enhanced to explicitly represent risk within a process. Secure*BPMN (Cherdantseva, 2014) was expanded by adding risk representation to it. The main processes in Information Security Risk Management (ISO 27005) were used as a basis to combine the Risk Register and Business Process Modelling as an approach to manage security risks. Managing Security Risk – Business Process Modelling (MSR-BPM) can manage risks by addressing visibility and shared awareness of risk. Also, it helps to identify different risks due to the context of the process.

The nature of the risks changes because modelling the process brings a stronger emphasis on the context of the risk. For instance, Chapter 5 provided a generic reference risk register table which holds most of the management perspectives areas. It holds change project risks, operational risks associated with central cloud infrastructure and operational risks associated with the hospital business processes.

However, the countermeasures provided are in general format. They need to be customised according to the context.

Chapter 6 discussed key aspects for using a use case scenario to model the current situation and a potential future situation using cloud computing. It represents how the nature of risks and the countermeasures required to mitigate these risks changed significantly as the context changed to cloud computing. For instance, it addressed physical data protection risks in the current situation, whereas in cloud computing it addressed governance issues such as GDPR compliance for protecting data in Germany, which is not used in Oman. In addition, migrating to HL7 to address interoperability issues was not identified in the generic reference risk register table in Chapter 5.

MSR-BPM approach is valuable to identify the risks in associated with using cloud computing to support healthcare processes. Considering risk management perspectives helped to identify the responsibility of different stakeholders for managing the risks, both inside and outside the scope of the hospital. MSR-BPM indicates the importance of using the process model and risk register to provide a clear understanding where the risks occur and how these need to be managed. For instance, at the operational level the hospital needs to manage risks such as Malicious insider, Identity access management and insecure deletion of data. Some of these risks and countermeasures change significantly when the context moves to cloud computing. For instance, for Data protection the patient needs to secure his PKI in Oman to prevent unauthorised access, whereas in Germany hospital, there is a need for GDPR compliance as patient needs to give consent for accessing his records. Applying MSR-BPM approach helped in understanding cloud computing context especially in providing the relevance of each risk to the healthcare context in Oman.

It can be challenging when modelling the process to decide the right level of abstraction, whilst ensuring that the diagram does not get too complex. The separation of concerns is recommended to model the infrastructure architecture (which is primarily the concern of ODP and ITA-Cloud) separately from the business

architecture (which is primarily the concern of the hospitals). It will create several benefits such as (a) the dimensions of risk will be reduced considerably (b) the diagrams are likely to be less 'busy'; (c) the extended risk register becomes simpler. This helps to focus on the risks that are pertinent to the architectural view. However, it is important to understand and manage the impact of any future changes on each of the architectural views.

Chapter 7 was used to evaluate the MSR-BPM approach with practitioners. There was a need for a realistic scenario to critically evaluate the MSR-BPM integrated approach at the operational level within a business process which deals with day-to-day operations. Integrated Care Pathway (ICP) for breast cancer was chosen as it shows the processes, roles, activities and different locations. It will not be evaluated in cloud as it is inappropriate to the context. However, the cloud context had been analysed in Chapter 5 and 6. The feedback from practitioners provided advantages and limitations of the MSR-BPM approach. They supported using the risk register with the business process model to understand risks, enhance effective communication, identify any change in risks as it proved helpful in structuring and organising risk-related information. It is also useful when there is a complicated process that handles multiple locations and stakeholders. However, there are limitations for using the MSR-BPM. First, it does not help to identify the most the appropriate countermeasure to mitigate the addressed risks. Second, it takes time to draw the BPM diagram. Third, it is challenging in terms of how much detail needs to be included in the BPM diagram. Furthermore, the user acceptance of the approach and the need to be familiar with BPM area is another concern because a clinician or a nurse might not be familiar with the modelling aspect nor have a detailed knowledge of the security issues and countermeasures.

The feedback from the evaluator of MSR-BPM confirms that the approach helps in visualising the operational risks with the hospital and assists in providing a risk register as a living document throughout a project, but it does not provide countermeasures. The stakeholder team needs to decide the suitable countermeasures needed according to the risk analysis.

7.6.7.4 Future Work

There is scope for further research regarding the MSR-BPM approach and that is to extend the method to address various types of risks (management, technical and legal) which were explored in Chapter 3. In addition, the research can be further developed through software to provide an automated detection and mitigating recommendations for similar risks rather than creating the tables manually. Therefore, it will not only detect such risks, but also provide comprehensive solutions as well.

Addressing Provenance will enhance the MSR-BPM approach to trace events in complex distributed processes. In addition, it will show dependencies between such events, and associated decisions by human actors.

There is also the need to provide a training session for using the MSR-BPM as some of the participants raised concerns regarding the use of the MSR-BPM by non-technical stakeholders. The training session would increase user awareness of the MSR-BPM approach and highlight how it differs from a traditional risk register by providing a living document of risks which can identify any changes within risks. In addition, enhancing employee awareness of security risks through regular and up-to-date workshops could reduce the security risks. This will therefore reduce the expense of mitigating critical risks.

Participant 6: *“Have the right methodology and tooling is essential for managing security risk. Having a methodology that is sound is good, and I think this can be used, but you would need to spend the time not just creating the method but also building the training and implementation capability, as people performing this work are incredibly busy and don’t always have time to learn new methods if the methods they are using are ‘good enough’ Being a better method is not always a good enough reason to stop doing what has been working, so you’ll need to construct a compelling reason not just why this is good, but also why the current method is not good.”*

The MSR-BPM can be linked with security systems to improve its effectiveness by assessing the countermeasure in mitigating the risks. If the countermeasure is not suitable, it will be modified accordingly.

Participant 11: “... *To be effective it would also need to be linked to the security system design documentation to measure how well the identified risks are mitigated (or not) as the systems capability (in terms of people, process and technology) change over time.*”

Also, Participant 12 is quite right in pointing out the need for a broader application to address various types of risks. Therefore, the MSR-BPM can be used in a broader context to address not only security risks but also management, technical and legal risks. It depends on the process that it is used for and how much detail the stakeholders’ team is required to gather during their discussion meeting.

Participant 12: “*Typically this approach will enable the identification of risks through a particular lens - in this case a process. However, security is somewhat all encompassing. Depending on the ultimate consumer of the activity, sticking to this approach will likely miss more binary risks driven by regulatory compliance; technical risk driven by more extensible systems and architectures (e.g. cloud infrastructure not managed by you) as well as contractual risk. I don’t know the overall objective so it’s hard to contextualise the question, so it may be appropriate, alternatively a broader approach may be required whereby this assessment can be used as part of a number of techniques to derive the overall risk posture.*”

This would be enabled using an enterprise architecture approach, as discussed in Section 6.5. However further work is needed to determine how an enterprise architecture approach such as TOGAF could be enhanced to manage risks across the different architectural concerns.

Multidisciplinary stakeholder teams can use the MSR-BPM to identify different types of risks, for instance, in terms of business continuity and management which include technical, management and security risks. The MSR-BPM can also potentially be

applied within other domains, such as the banking sector, telecommunications, airlines or education, to provide effective communication on information security risks.

In addition, the MSR-BPM approach is used in this research at an operational level within a business context. In future, the approach can be used in a broader context within a strategic level within models and ISO 31000. Further work can consider using the Risk Register with BPM in conjunction with the ISO 31000 to effectively manage organisational policy and strategy level. Thus, risks can be managed across the organisation. It can identify technical risks and security risks as well as other risks identified from the perception such as managerial, legal and clinical risks.

Oman is currently not applying the risk management approach in healthcare, which provides a barrier to the adoption of the MSR-BPM approach. However, organisations that are familiar with the ISO 27000 standards in Oman, such as Information Technology Authority (ITA), can potentially adopt the MSR-BPM approach because they are already using the ISO 27000 in their workplace. The MSR-BPM approach can be used in the UK as participants view the Risk Register as a living document in the evaluation experiment. The Risk Register is widely adopted in the healthcare domain in the UK.

7.7 Conclusion

This chapter presented an evaluation of the MSR-BPM within a complicated healthcare scenario through the Integrated Care pathway for breast cancer. The scenario was chosen because it had been used by several researchers within the Computer Science and Informatics Department at Cardiff University. It presents a complex treatment pathway which includes multiple locations and multiple stakeholders.

Although other researchers addressed important concerns, such as information-sharing between GPs and members of the cancer team (Allam, 2006), automated workflow between the users of CISs and the legacy systems (Alsalamah,H. 2012), controlling

access permission between different locations (Burnap et al., 2012) and security requirements of the patient-centric approach (Alsalamah, S.2014), their research did not address information security risk in the healthcare processes.

The literature on quality evaluations and quality standards was reviewed to determine a set of criteria to evaluate the MSR-BPM approach. It was important to ensure that the right quality criteria were involved in the evaluation of the approach to determine the effectiveness of the proposed MSR-BPM approach in enhancing the communication of information security risk in the healthcare process through survey questions.

The feedback from the participants of the survey revealed both advantages and limitations of using in MSR-BPM approach:

- The evaluators are in strong agreement regarding using MSR-BPM approach in establishing the context as they found it useful and effective in understanding the risks.
- They support combining the risk register with business process modelling because it clearly identifies risks and enhances the traceability of risk in a complex process with multiple locations and stakeholders.
- MSR-BPM can help in identifying any changes within risks rather than using a risk register only.
- MSR-BPM approach proved that it could provide effective communication of information security risks in healthcare processes by combining risk register and business process modelling to visualise risks in healthcare processes and providing a shared understanding of these risks for stakeholders.

In terms of limitations, the evaluators indicated uncertainty regarding whether the MSR-BPM approach would be useful in determining the countermeasures to mitigate the risks. This relies on the expertise of the stakeholder carrying out the analysis. However, the MSR-BPM can be useful in the planning phase to document the countermeasure once they are determined.

In addition, the MSR-BPM approach was reflected upon according to the ISO 27005 processes to consider its effectiveness, advantages, limitations and suggestions for future work that could be carried out based on areas identified by this research that will be worth further investigation.

The next chapter will highlight the key aspects of the research, before drawing conclusions

8 Chapter 8: Conclusion

8.1 Introduction

This chapter summarizes the key aspects of the research. It discusses the achievements of the research against its aims and objectives, draws conclusions from this research and confirms the research hypothesis. This chapter concludes with a summary of the originality and significance of the research contribution to learning.

8.2 Achievements of the Research Objectives

Section 1.2 identified the objectives that needed to be satisfied in order to achieve the research aim to develop a methodology to manage risks in order to improve the communication of Information Security Risk in the healthcare processes. These are reviewed in this section.

8.2.1 Research Objective One

Survey the literature to understand the benefits, challenges and risks associated with utilising cloud computing in healthcare and its relevance to the healthcare context in Oman

Chapter 2 provided a background of cloud computing. It also addressed the benefits of using cloud computing in healthcare, providing different examples. Having cloud computing as a potential solution to address healthcare limitations requires a deep understanding of cloud computing benefits, challenges and risks associated with it. Therefore, a strategic analysis was performed of using cloud computing in the healthcare by observing the benefits and performing a SWOT analysis to understand the internal and external factors affecting cloud computing's adoption. It was found that there are significant risks that need to be managed. Cloud computing risks in significant areas, such as management, technical, legal and security areas, were examined to gain a holistic view of risks that need to be considered before the adoption process.

Table-2-3 presented risk register to summarise the main risks found in the literature. The risk register was expanded to highlight the importance and relevance to the

healthcare context in Oman. Also, it identified some of the operational risks associated with central cloud infrastructure managed by the ODP and ITA-Cloud.

In Chapter 5 the generated reference risk register table came from combining standards such as ISO 27005 and ENISA with the Omani context. It indicated different ranges of risk types and countermeasures, which are needed to reduce the risk level. It identified 46 risks with appropriate countermeasures, security goals and risk levels. The use of cloud computing as a potential solution was explored in the hypothetical scenario in Chapter 6 to ease the exchange of sensitive data between two different countries. In addition, MSR-BPM was used to model the process of the scenario and generate a risk register with Strategic, Change and Operational risks specific to the context. The risk registers generated in chapters 2, 5 and 6 will assist stakeholders in mitigating the identified risks in a change project to expand cloud computing to enable the sharing of patient records, and in managing risks associated with using cloud-computing in the hospitals' operational processes.

It can therefore be concluded that the first objective was achieved and an understanding was gained in terms of the benefits, challenges and risks associated with utilising cloud computing in the healthcare and how this relates to the Omani context (Table-2-3).

8.2.2 Research Objective Two

To understand stakeholders' perceptions of risks in utilising cloud computing in the delivery of healthcare services

Based on the comprehensive knowledge gained from Chapter 2 regarding cloud computing, preliminary interviews with seven stakeholders were designed. In addition, two sets of questionnaires (400 for the public and 150 for healthcare professionals) were provided to understand the perceptions of stakeholders.

The questions of the public and healthcare professionals' questionnaires were adopted from Lian et al. (2014), Wijaya et al. (2014), Singh et al. (2014) and Chang et al. (2007). The questionnaires asked a very broad range of questions (75 questions) about the perceptions of risks in different areas, such as human, privacy, technology, organisational and environmental areas. The reliability and validity of the questions were checked through factor loading and Cronbach's Alpha. Through the process, some of the questions were dropped. 46 questions were used for the analysis. The SPSS analysis and Radar Charts provided a detailed analysis of the various types of risks concerning human, privacy, technology, organisational and environmental areas. It was found that the major concerns were Data Security, Confidentiality, Integrity and Availability. Therefore, the findings emphasize the need for an effective methodology to manage such risks. The findings were validated with the Undersecretary for Planning Affairs in Ministry of Health who confirmed the need to have an effective methodology to manage risks within cloud computing.

The key deliverables of Chapter 3 represent comprehensive statistical information about the stakeholder perception of different types of risks (Security, Management, Technical, Legal and other types of risks) that affect adopting cloud computing as a service. In addition, this research contributes to the literature by highlighting the risk factors preventing the government from adopting cloud computing as a service in the healthcare industry in the Omani context. Therefore, the second objective was achieved and a deeper understanding of stakeholders' perceptions of risks in utilising cloud computing in the delivery of healthcare services was obtained.

8.2.3 Research Objective Three

Understand the framework and techniques used to manage risks and business process modelling to visualise risk.

Chapter 4 provided a literature review on managing information security risk in general. The ISO/IEC 38500 for Corporate Governance of Information Technology was addressed. Risk Management (ISO 31000) was studied to understand the

techniques and guidelines of managing risks. Information Security Management Systems (ISO 27000) and Information Security Risk Management (ISO 27005) were discussed. A critical analysis of the ISO 38500, ISO 31000 and ISO 27000 methods were conducted and a comparison between the methods was carried out to be aware of how each method works, how it is used, which ISO it has compliance with, advantages, limitations and the technique it uses to manage risks. A summary table of the comparisons was created. Similarly, a comparison of the different tools that are commonly used within the healthcare industry to manage risks was considered. Risk Register (RR), Operational Critical Threat and Vulnerability Evaluation (OCTAVE) and Failure Modes and Effect Analysis (FMEA) are the commonly used methods.

A comparison table between OCTAVE, Risk Register and FMEA based on the ISO 27005 processes was created. OCTAVE is an evaluation activity where a team identifies risks, analyses them to determine priorities and plan for improvement by developing a protection strategy for organizational improvement and risk mitigation plans to reduce the risk to the organization's critical assets. It is not a continuous process as it has a defined beginning and end. FMEA is an assessment tool, but it does not eliminate risks. Although FMEA was useful as a risk analysis tool, it has many limitations, such as being biased toward severity ratings, having an ever-increasing list of possible failure modes, and being only as effective as the how the members of the FMEA team are using it.

A risk register documents the assessment of risk with appropriate countermeasures; it is fully covered by Information Security Risk Management's (ISO 27005) main processes. Therefore, the key significant deliverables are based on choosing risk register as the most appropriate tool for addressing risks. However, there are limitations related to using the risk register as it lacks visibility of the process and lacks a shared understanding of risks associated with each role. Thus, there is a need to enhance the risk register document through visualising the whole process, especially when there is a complicated process, which includes roles, processes, activities and multiple locations when different organisations are involved.

In addition, information security literature was examined to understand the concept of information security. The role of process modelling prospected in risk management framework was considered. Business Process Modelling (BPM) is a commonly used method in modelling techniques. The graphical style of the BPM furthers communication and interaction between stakeholders involved in a risk assessment. It was found that there was a better understanding of the risks through enhancing the communication of the risks in process modelling. However, the BPM does not provide the details of the countermeasure needed to manage the risks. Thus, there is a need to link it with another tool which can address this limitation.

Therefore, the third objective of understanding the framework and techniques used to manage risks and business process modelling to visualise risk was achieved.

8.2.4 Research Objective Four

Develop an approach to address the stages of ISO 27005 and determine how to combine risk register and business process model to communicate information security risks

Chapter 5 presented three contributions of this research. The first contribution relates to creating a comprehensive - and enhanced beyond previous work - generic reference risk register ([Appendix C](#)) which includes a mixture of risk management perspectives risks. It includes: Change project risks associated with introducing cloud computing into the hospital, Operational risk associated with central cloud infrastructure managed by the ODP and ITA-Cloud and Operational risks with the hospital. RMIAS (Cherdantseva, 2014) was used as a basis to create the risk register table and added traceability to show the risk location within a complex process. Many of the risks are out of scope of the hospital and are managed in the Change Project to transition to cloud or are managed by the ODP/ITA.

The second contribution centres on providing an extension for Secure*BPMN to explicitly represent risk in the BPM. Secure*BPMN (Cherdantseva, 2014) was used as a strong candidate for modelling security concerns because it is accessible by all members of a multidisciplinary team, irrespective of their area of expertise. The syntax

of Secure*BPMN was designed specifically for human understanding and communication improvement purposes (Cherdantseva, 2014). Due to the researcher's lack of familiarity with business process modelling, challenges were faced when using the modelling technique. In addition, choosing the risk symbol was difficult, as it had to be clear to the public who come from different backgrounds. Therefore, a triangle shape that was designed based on the road hazard symbols was used because it is deemed to be the most familiar to people who come from different backgrounds.

The third is the main contribution of this research. It focuses on developing an approach, Managing Security Risk–Business Process Modelling (MSR-BPM), to visualise risks in a healthcare process and promote a shared understanding of the risks for stakeholders by combining risk register and business process modelling. A risk register documents the assessment of risk with appropriate countermeasures. The BPM visualises the risk activities, security goals and countermeasures in the process models to promote a shared understanding of risks to decision makers and stakeholders.

It was decided to enhance the usefulness of the risk register by combining it with a business process modelling based on the ISO 27005 processes to show the anticipated benefits, as outlined in section 5.4. [Table 5-12](#) showed that the risk register and business process modelling complement each other effectively. They provide a shared understanding of risks and improve the communication of information security risks in the healthcare process in complex processes with multiple locations and stakeholders. Also, the MSR-BPM is enriched with stakeholder perceptions of risks. The key deliverables of Chapter 5 featured presenting a methodology MSR-BPM approach to manage risks within a process.

The MSR-BPM approach is different from other approaches. Other researchers used risk modelling in an algorithmic or quantitative approaches to risk, whereas the MSR-BPM uses a qualitative approach and focuses on representing risk within the Business Process Modelling, ensuring that it is linked with the risk register to document the risk assessment.

Therefore, by developing the MSR-BPM approach to follow the stages of the ISO27005 Information Security Risk Management Process and determining how to combine both the risk register and business process model to communicate the information security risks, the fourth objective was achieved.

8.2.5 Research Objective Five

Identify a healthcare scenario to explain the need for migrating healthcare services to cloud computing and apply the approach to the scenario

Chapter 6 addressed the application of the MSR-BPM approach through a hypothetical case study scenario that had been used in the preliminary interview to demonstrate the need for an improved communication mechanism in healthcare. It showed the benefit of having patients' records available online to avoid multiple tests as well as having collaboration and communication between healthcare institutions in different locations. Having cloud computing may be considered as a solution but there are risks associated with it. The focus of this research was the security risks.

This research followed the MSR-BPM stages as shown in [Figure 5-3](#) in Chapter 5 to present the application in two ways: from a research approach to discuss how the scenario was modelled and from an anticipated stakeholder perception. The ISO 27005 Information Security Risk Management Process was followed at each stage in detail, which helped to structure the thinking about the security risks and to ensure that each activity in the process had been addressed. The ISO 27005 was chosen as it is an international information security standard which is widely used to manage risks. The MSR-BPM approach highlights the importance of enhancing the use of a risk register with business process modelling to provide a more effective way of communicating risks. In addition, it shows the importance of combining the risk register with business process modelling as a way to communicate risks. It presents the importance of visualising risks for decision makers and stakeholders. Also, it

highlights the importance of enriching the situation by involving stakeholders and multi-disciplinary team perceptions. Hence, the risks are made obvious to all stakeholders who have different perceptions of risks that need to be discussed openly when applying the MSR-BPM approach.

It is challenging to include every step that a patient goes through; it will cause inconsistency over time as multidisciplinary teams will have different ideas regarding how the process should be carried out. As a consequence, there could be different processes with different activities and there will be different risks encountered too. It makes more sense to have a subprocess with risks which identifies the locations. The use of a subprocess for common processes can help in situations where both models become over complicated. In addition, the subprocess can facilitate obtaining more consistency when these activities are carried out in different locations. Therefore, the common processes need to model separately.

The process model can become very complicated, particularly when looking at technology solutions. If it is likely that the same technology solution will be used for different pathways and different approaches, then it makes sense to manage the IT Infrastructure Risks separately from The strategic risks which covers governance aspects, project risks which handle the migration to cloud computing and operational risks which covers day-to-day activities in hospital level. ODP and ITA-Cloud would manage many of IT infrastructure cloud computing risks centrally.

Chapter 6 discussed key aspects for using a use case scenario to model the current situation and a potential future situation using cloud computing. It represents how the nature of risks and the countermeasures required to mitigate these risks changed significantly as the context changed to cloud computing. For instance, it addressed physical data protection risks in the current situation, whereas in cloud computing it addressed governance issues such as GDPR compliance for protecting data in Germany, which is not used in Oman. In addition, migrating to HL7 to address interoperability issues was not identified in the generic reference risk register table in

Chapter 5. MSR-BPM approach is valuable to identify the risks in associated with using cloud computing to support healthcare processes. Considering risk management perspectives helped to identify the responsibility of different stakeholders for managing the risks, both inside and outside the scope of the hospital. MSR-BPM indicates the importance of using the process model and risk register to provide a clear understanding where the risks occur and how these need to be managed

Section 6.4 considered the use of cloud computing as a potential solution to facilitate communication between different locations and enhance the collaboration between different stakeholders. It was found that the choice of technology that was used to share information across different locations has a significant impact on the risks that will be faced. Also, it was suggested that cloud computing was a potential technology solution which may facilitate communication among different locations as well as address other types of risks. However, stakeholders need to discuss all the potential risks openly to determine which technology solution they should implement within their organisation.

The key deliverables of Chapter 6 were related to identifying the practical use of the MSR-BPM approach through a hypothetical scenario. Therefore, the fifth objective was achieved in using an approach to document and visualise security risks and countermeasures in a healthcare scenario that benefits from cloud computing.

8.2.6 Research Objective Six

Evaluate the proposed approach with experts across the field of Risk management, Business process management and Healthcare through the Integrated Care Pathway scenario.

Chapter 7 aimed to evaluate the MSR-BPM approach through a more complex scenario for breast cancer in the UK. The scenario was chosen because it had been used in various research papers within Computer Science and Informatics at Cardiff University. It presented how complex the treatment pathway is in reality in that it

includes multiple locations and multiple stakeholders. An evaluation methodology was created based on the ISO 27005 activities in the Information Security Risk Management Process to create survey questions for experts in Risk Management, Business Process and Healthcare. The survey was divided into three sections, participant profile, evaluating the MSR-BPM approach usefulness and qualitative feedback, to provide a greater insight into the effectiveness of the approach. Twelve individuals from the UK participated in the empirical evaluation of the MSR-BPM. They had high-level expertise in risk management (7) and business process modelling (6). Several were familiar with the healthcare industry (6).

This research aimed to establish the extent to which the MSR-BPM approach was useful and effective in understanding the risks. The feedback from the evaluators supported using the risk register with the business process model as a way to understand risks and to enhance communication among stakeholders. Also, they were in strong agreement that the MSR-BPM approach can identify any change in risks rather than using the risk register only. In addition, they pointed out that the MSR-BPM is helpful in structuring and organising risk-related information. The MSR-BPM approach is useful when there is a complicated process that handles multiple locations and stakeholders because it can identify the risks in each process as well as allow team members to discuss each risk impact, likelihood and level rather than copying information from the previous risk register document. Thus, the risk register document will be a living document.

The MSR-BPM approach has a substantial importance in providing a shared understanding of risks holistically among stakeholders and enhancing communication between different locations, as the scenarios used for applying the approach (Chapter 6) and evaluating the approach (Chapter 7) span multiple locations. In addition, it enhances traceability of risk changes. Therefore, the MSR-BPM approach helps in the Monitoring and Review process by identifying which activities, roles and locations may be affected by any changes within risks rather than using the risk register only. The BPM diagram will update the process to clearly visualise the risk, whether at the process level or activity level.

Therefore, the results of the evaluation have proved the research hypothesis that the communication of information security risk in healthcare processes can be improved by combining the risk register and business process modelling to achieve a shared understanding of risks and visualize the risks for decision makers and stakeholders. However, experts observed that MSR-BPM has several limitations. Firstly, although it can document the chosen countermeasure in the risk register, it does not help to identify the most appropriate countermeasure to mitigate the addressed risks. Another limitation is that it takes time to draw the BPM diagram. It is challenging in terms of how much detail needs to be included in the BPM diagram. Furthermore, the user acceptance of the approach and the need to be familiar with the BPM area is another concern because a clinician or a nurse might not be familiar with the modelling aspect nor have a detailed knowledge of the security issues and countermeasures. It is recommended that the MSR-BPM is applied with a multi-disciplinary team with relevant stakeholders, including a business analyst and security expert. This may be difficult to achieve in practice and it will represent an obstacle in using the approach.

In addition, Chapter 7 aimed to evaluate the MSR-BPM approach among stakeholders in Oman and the UK. In the UK, the proposed approach was evaluated through an Integrated Care Pathway (ICP) scenario which holds multiple locations and stakeholders. The practitioners agreed that MSR-BPM approach can provide effective communication of information security risks. 75 percent identified that the approach is clearly understandable and appropriate to use to manage security risk in healthcare processes. In addition, 91 percent agreed that the MSR-BPM is more likely to effectively communicate risks to achieve a shared understanding of all roles involved in the process compared to using a risk register only. Also, 82 percent pointed out that the MSR-BPM is more likely to help healthcare organisations manage security risks in compliance with Information security risk management practices (ISO27005) compared to developing a Risk register only.

Unfortunately, there was a lack of responses among stakeholders in Oman. The lack of adoption of Risk Registers in the healthcare in Oman would be a barrier to migrating MSR-BPM approach in the Omani context. In addition, this lack of risk management awareness caused an obstacle to evaluate the MSR-BPM approach within

Omani context. However, the MSR-BPM is suitable for any organisation familiar with the ISO 27000 standards and could be adapted with further research for organisations that are familiar with the ISO 31000 standards.

The Omani healthcare system has not yet adopted the concept of patient pathways. Oman has extensive plans to strategically implement initiatives to make health care systems “patient-centred” (WHO, 2017). If Oman moves to patient-centred system, MSR-BPM approach will help in providing shared understanding of anticipated risks during patient pathways.

The sixth objective has been achieved in the UK context through the evaluation of the MSR-BPM approach. However, it is not been possible to evaluate this approach in the Omani context as risk registers are not used in the health care sector.

Therefore, the research hypothesis was fulfilled and the communication of Information Security Risk in Healthcare processes can be improved by combining the risk register and business process modelling to visualise risks in a complex and significant healthcare process, such as the Integrated Care Pathway for Breast Cancer, and achieve a shared understanding of these risks for stakeholders

8.3 Originality and Significance of Research Contribution

1. Provides comprehensive and significant statistics about the perception of different types of risks (Security, Management, Technical, Legal, Privacy and other types of risks) in adopting cloud computing as a service in the delivery of healthcare services within the Omani context. The results have enhanced the understanding of the perceptions of risks in the current system and cloud computing in the healthcare industry in Oman.

2. Created a comprehensive - and enhanced beyond previous work - generic reference risk register for migrating cloud computing in healthcare. This research has added to the available literature concerning various types of risks in the current system and cloud computing in healthcare. The generic reference risk register table lists the risk name, risk description, risk impact, risk likelihood, risk level, security goal and countermeasure. Therefore, it enriches understanding, within the context of Oman, of security, management, technical and cloud computing risks in the healthcare.

3. Provides an extension to Secure*BPMN (Cherdantseva, 2014) by adding a risk representation to it. The decision makers and stakeholders team need to visualize the risks in the BPM diagram to gain a holistic view of the associated risks. The approach in this research is different as it focuses on representing risk explicitly within the BPM. Other researchers discuss integrating security requirements to the BPM (Rodríguez et al., 2007), extending the BPMN with a set of security concepts for Service-Oriented Architecture (SoA) applications (Saleem et al., 2012), SecureBPMN (2012) extending the BPMN with access control and information flow constraints (Salnitri et al., 2017) and Secure*BPMN for communicating Information Assurance and Security (IAS) concepts to business experts and other non-technical audiences. Secure*BPMN added additional security classes such as Secure Swimlane, Secure Swimlane location, Access Permission, Information Taxonomy, Security Goals and Countermeasures, but did not represent or model risk. Conforti (2014) developed an operational approach for the management of risks related to executable business processes in near real-time. Jakoubi et al. (2010) presented a methodology enabling the risk-aware modelling and simulation of business processes in an algorithmic way while Koster (2009) proposed an evaluation method for Business Process Management products. Therefore, these researchers focused on quantitative methods to evaluate risks rather than on qualitative methods to represent risks and this is how the proposed approach in this research is different.

4. The main contribution of this thesis is the creation of the MSR-BPM approach as an integrated approach to manage security risks. There are existing techniques which can be used for managing information security risks that are centred around the ISO 27000. The ISO 27000 helps in managing security risks in the UK which uses risk register, but it does not include people and processes within it. There are other techniques for modelling security concerns such as Secure*BPMN. Secure*BPMN helps to identify security concerns within processes as it links people and processes to information security countermeasures and information security goals. However, it does not include risk register or explicitly represents risks. Hence, the integration of the ISO 27000 and Secure*BPMN helps to create an integrated approach: the MSR-BPM. The novelty of the MSR-BPM is combining a risk register, Secure *BPMN and visualisation of risks on a graphic of Business Process. It supports all aspects of operational services in day-to-day activities which include people, processes and information security. The MSR-BPM is very important to visualise risks in a healthcare processes and promote a shared understanding of the risks to stakeholders. This view was supported by the evaluation of healthcare practitioners who are in broad agreement that MSR-BPM is more likely to effectively communicate risks to achieve a shared understanding of all roles involved in the process compared to using a risk register only. Also, most of them agreed that the MSR-BPM is more likely to help healthcare organisations manage security risks in compliance with Information security risk management practices (ISO27005) compared to developing a Risk register only.

In terms of the contribution of this research in relation to the literature, many methods based on the ISO 27000 were discussed in Chapter 4 section 4.6. Organisations can use the ISO 27000 methods, but the MSR-BPM provides a better modelling process as it identifies the risk location in each process and provides a shared understanding of risks for stakeholders. According to the ISO 27000 methods, such as NIST, EBIOS, MEHARI, MAGERIT and CORAS, each method manages risks through risk identification, risk analysis, risk assessment, risk treatment and risk evaluation. NIST provides the information and communication flows necessary to make the process work effectively. The proposed approach in this research, the MSR-BPM, is not a replacement for those

methods, but rather it is a technique which can be used in conjunction with these methods to provide a better output by providing a risk register and risk representation in the BPM. The MSR-BPM is compliant with the ISO 27005 processes. Other risk management tools do not have the same presentation that the MSR-BPM provides. For instance, OCTAVE and FEMA do not provide monitoring and review or communication and consultation for the whole process. OCTAVE is more likely helpful in the plan phase and FEMA is more likely to be used as an analysis tool. The MSR-BPM is compliant with the ISO 27000 as it focuses on risk assessment. Also, it has compliance with the ISO 27005 stages. The MSR-BPM approach followed the ISO 27005 processes for establishing the context from risk register and business process models. It is based on the best practices in information security risk management in healthcare process as it is grounded in the ISO 27005 processes. The evaluation in Chapter 7 shows the effectiveness of the MSR-BPM in improving the communication of information security risks in healthcare processes. Therefore, the MSR-BPM approach helps to improve the communication of information security risk management in healthcare processes by following the ISO 27005 processes:

- Establishing context to show the current situation. It is necessary to collect all information about information security risk management and which requirements need to be addressed by understanding the staff roles and locations. Staff can gain a shared understanding of risks in the process. Therefore, it facilitates the reporting and communication of risks within an organisation.
- Risk assessment through risk identification, risk level, likelihood and impact. The BPM diagram will visualize the risks in different stages, such as process, activities and flow dependency.
- Risk treatment through documenting the appropriate countermeasure type in the BPM and detailing discussion within risk register table.

- Monitoring and reviewing by adding the traceability column to the risk register document to clearly show the position of risk, whether it is in a process, activity or flow. It is suggested that the domain provenance can be addressed in future research. Provenance information can be a resource for “reflection-in-action” during analysis, supporting collaboration between analysts, and helping to trace data quality and uncertainty through the analysis process. It can also act as a resource after the event, supporting the interpretation of claims, audit, accountability, and training.

- Communication and consultation by providing an agreement on how to manage risks by exchanging and sharing information about risk among decision makers and stakeholders.

9 References

References:

- Aagedal, J.O., Den Braber, F., Dimitrakos, T., Gran, B.A., Raptis, D. and Stolen, K., 2002. Model-based risk assessment to improve enterprise security. In Enterprise Distributed Object Computing Conference, 2002. EDOC'02. Proceedings. Sixth International (pp. 51-62). IEEE.
- AbuKhoua, E., Mohamed, N. and Al-Jaroodi, J., 2012. e-Health cloud: opportunities and challenges. *Future Internet*, 4(3), pp.621-645.
- Aguilar-Saven, R.S., 2004. Business process modelling: Review and framework. *International Journal of production economics*, 90(2), pp.129-149.
- Aguilar-Saven, R.S., 2004. Business process modelling: Review and framework. *International Journal of production economics*, 90(2), pp.129-149.
- Ahuja, S. P., Mani, S., & Zambrano, J. (2012). A survey of the state of cloud computing in healthcare. *Network and Communication Technologies*, 1(2), p12.
- Akhtar, M.F., Ali, K. and Sadaqat, S., 2011. Liquidity risk management: a comparative study between conventional and Islamic banks of Pakistan. *Interdisciplinary Journal of Research in Business*, 1(1), pp.35-44.
- Al-Ahmad, W. and Mohammad, B., 2012. Can a single security framework address information security risks adequately?. *International Journal of Digital Information and Wireless Communications (IJDIWC)*, 2(3), pp.222-230.
- Alam, M.G.R., Cho, E.J., Huh, E.N. and Hong, C.S., 2014, January. Cloud based mental state monitoring system for suicide risk reconnaissance using wearable bio-sensors. In Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication (p. 56). ACM.
- Alberts, C., Dorofee, A., Stevens, J. and Woody, C., 2003. Introduction to the OCTAVE Approach. *Pittsburgh, PA, Carnegie Mellon University*.
- Alberts, C.J., Behrens, S.G., Pethia, R.D. and Wilson, W.R., 1999. Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, Version 1.0.
- Alkhater, N, Walters, R. and Wills, G., 2017. An empirical study of factors influencing cloud adoption among private sector organisations. *Telematics and Informatics*.
- Allam, O. (2006). A Holistic Analysis Approach to Facilitating Communication between General Practitioners and Cancer Care Teams. PhD. Cardiff University.
- Alruwaili, F.F. and Gulliver, T.A., 2015. Secsdlc: A practical life cycle approach for cloud-based information security. *IJRCCT*, 4(2), pp.095-107.

- Alsalamah, H. (2012). *Supporting Integrated Care Pathways with Workflow Technology*. PhD. Cardiff University.
- Alsalamh, S. (2014). *Achieving a Secure Collaborative Environment in Patient-Centred Healthcare with Legacy Information Systems*. PhD. Cardiff University.
- Alshaikh, M., Ahmad, A., Maynard, S.B. and Chang, S., 2014. Towards a taxonomy of information security management practices in organisations. ACIS.
- American Society for Healthcare Risk Management, 2011. *Risk Management Handbook for Health Care Organizations, 3 Volume Set*. John Wiley & Sons.
- Amini, A. and Jamil, N., 2018, May. A Comprehensive Review of Existing Risk Assessment Models in Cloud Computing. In *Journal of Physics: Conference Series* (Vol. 1018, No. 1, p. 012004). IOP Publishing.
- Anderson, J. 2003. "Why we need a new definition of information security," *Computers & Security*, 22(4) pp. 308-313.
- Armbrust, M., Fox, O., Griffith, R., Joseph, A. D., Katz, Y., Konwinski, A. & Zaharia, M. (2009). M.: Above the clouds: a Berkeley view of cloud computing.
- Assunção, M.D., Calheiros, R.N., Bianchi, S., Netto, M.A. and Buyya, R., 2015. Big Data computing and clouds: Trends and future directions. *Journal of Parallel and Distributed Computing*, 79, pp.3-15.
- Astuti, H.M., Muqtadiroh, F.A., Darmaningrat, E.W.T. and Putri, C.U., 2017. Risks Assessment of Information Technology Processes Based on COBIT 5 Framework: A Case Study of ITS Service Desk. *Procedia Computer Science*, 124, pp.569-576.
- Awan, M.S.K., Burnap, P. and Rana, O., 2016. Identifying cyber risk hotspots: A framework for measuring temporal variance in computer network risk. *computers & security*, 57, pp.31-46.
- Bamiah, M., Brohi, S. and Chuprat, S., 2012, December. A study on significance of adopting cloud computing paradigm in healthcare sector. In *Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on* (pp. 65-68). IEEE.
- Barry LJ. (1995) Assessing risk systematically. *Risk Management* 42:12–17.
- Barua, M., Liang, X., Lu, R. and Shen, X., 2011. ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing. *International Journal of Security and Networks*, 6(2-3), pp.67-76.

- Blank, R.M. and Gallagher, P.D., 2012. Nist special publication 800-30 revision 1 guide for conducting risk assessments. *National Institute of Standards and Technology, Tech. Rep.*
- BS EN ISO 9001:2015 Quality Management Systems Requirements.
- BS ISO/IEC 25010:2011 Systems and software engineering - Systems and Software Quality Requirements and Evaluation (SQuARE) - System and software quality models.
- BSA, 2019. The Software Alliance. GLOBAL computing Scorecard- Germany 2019 https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Germany.pdf [Accessed on June, 2019]
- Budgen, D., Rigby, M., Brereton, P. and Turner, M., 2007. A data integration broker for healthcare systems. *Computer*, 40(4).
- Burnap, P.R., Spasic, I., Gray, W.A., Hilton, J.C., Rana, O.F. and Elwyn, G., 2012, May. Protecting patient privacy in distributed collaborative healthcare environments by retaining access control of shared information. In 14th International Conference on Collaboration Technologies and Systems (CTS), 2012, (Denver), pp. 490–497, IEEE.
- Butt A, Hameed S (2011) Success of Spiral Model along with its Development Techniques. Models and methods applied in sciences.
- Buyya, R., Beloglazov, A., & Abawajy, J. (2010). Energy-efficient management of data center resources for cloud computing: a vision, architectural elements, and open challenges. *arXiv preprint arXiv:1006.0308*.
- Cardiff and Vale University Hospital (2017) accessed on 18.05.2017 URL: <http://www.cardiffandvaleuhb.wales.nhs.uk/home>
- Carneal, G., J.D , Daviss,S. and Harbin, H., 2017. New Technologies for Improving Behavioral Health.
- Carter R, Hancock T, Morin JM, Robins N. (1995) Introducing RIKSKMAN Methodology. 1st ed.UK:NNC Blackwell Ltd.
- Catteddu, D. & Hogben, G. (2009), Cloud Computing: Benefits, Risks and recommendations for information security, Technical Report, European Network and Information Security Agency (ENISA).
- Chahino, M. and Marchant, J. (2010) CIS conference presentation, Washington DC.
- Chang, I. C., Hwang, H. G., Hung, M. C., Lin, M. H., & Yen, D. C. (2007). Factors affecting the adoption of electronic signature: Executives' perspective of hospital information department. *Decision Support Systems*, 44(1), 350–359.

- Chapman, C. and Ward, S., 2003. *Project risk management: processes, techniques, and insights*. Wiley.
- Cherdantseva, Y. and Hilton, J., 2013, September. A reference model of information assurance & security. In *Availability, reliability and security (ares), 2013 eighth international conference on* (pp. 546-555). IEEE.
- Cherdantseva, Y., 2014. Secure* BPMN-a graphical extension for BPMN 2.0 based on a reference model of information assurance & security. PhD Thesis, Cardiff University.
- Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K., (2016). A review of cyber security risk assessment methods for SCADA systems. *computers & security*, 56, pp.1-27.
- Chiarini, A., 2012. Risk management and cost reduction of cancer drugs using Lean Six Sigma tools. *Leadership in Health Services*, 25(4), pp.318-330.
- Chin, W. W. (2010) 'How to Write up and Report PLS Analyses' Handbook of Partial Least Squares: In: Esposito Vinzi, V.; Chin, W.W.; Henseler, J.; Wang, H. (Eds.). *Handbook of Partial Least Squares: Concepts, Methods and Applications* (Springer Handbooks of Computational Statistics Series, vol. II). pp. 713-735 Heidelberg, Dordrecht, London, New York: Springer.
- Choo, K.K.R., Heravi, A., Mani, D. and Mubarak, S., 2015. Employees' Intended Information Security Behaviour in Real Estate Organisations: a Protection Motivation Perspective.
- Chow-White, P.A., MacAulay, M., Charters, A. and Chow, P., 2015. From the bench to the bedside in the big data age: ethics and practices of consent and privacy for clinical genomics and personalized medicine. *Ethics and Information Technology*, 17(3), pp.189-200.
- Coleman, J., 2004, June. Assessing information security risk in healthcare organizations of different scale. In international congress series (Vol. 1268, pp. 125-130). Elsevier.
- Conforti, R., 2014. *Managing risk in process-aware information systems* (Doctoral dissertation, Queensland University of Technology).
- Davies, J.M., 1996. 7 Risk assessment and risk management in anaesthesia. *Bailliere's Clinical Anaesthesiology*, 10(2), pp.357-372.
- Davis, F.D., 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, pp.319-340.

- DeRosier, J., Stalhandske, E., Bagian, J.P. and Nudell, T., 2002. Using health care failure mode and effect analysis™: the VA National Center for Patient Safety's prospective risk analysis system. *The Joint Commission journal on quality improvement*, 28(5), pp.248-267.
- Desai, S.S., Dua, A., Kuy, S. and Upchurch, G.R., 2014. PS132. Mitigating Mortality in Abdominal Aortic Aneurysmal Disease Through the Use of a Risk Register: Indications for EVAR vs Open Repair. *Journal of Vascular Surgery*, 59(6), pp.65S-66S.
- Devadass, L., Sekaran, S.S. and Thinakaran, R., 2017. CLOUD COMPUTING IN HEALTHCARE. *International Journal of Students' Research in Technology & Management*, 5(1), pp.25-31.
- Dibbern, J., Goles, T., Hirschheim, R., & Jayatilaka, B. (2004). Information systems outsourcing: a survey and analysis of the literature. *ACM SIGMIS Database*, 35(4), 6-102.
- España, S., Condori-Fernandez, N., González, A. and Pastor, Ó., 2010. An empirical comparative evaluation of requirements engineering methods. *Journal of the Brazilian Computer Society*, 16(1), pp.3-19.
- European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry, (2012) COCIR eHEALTH TOOLKIT: Advancing healthcare delivery with cloud computing [Accessed on 25-05-2015] http://www.cocir.org/fileadmin/4.4_eHealth/eHealth_Toolkit_INT_2012_chap2.pdf .
- European Union Agency for Network and Information Security (ENISA) 2018 https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ramethods/m_ebios.html[Accessed on 1-06-2016]
- Fabian, B., Gürses, S., Heisel, M., Santen, T. and Schmidt, H., 2010. A comparison of security requirements engineering methods. *Requirements engineering*, 15(1), pp.7-40.
- Finne, T., 2000. Information systems risk management: key concepts and business processes. *Computers & Security*, 19(3), pp.234-242.
- Gillies, A., 2011. Improving the quality of information security management systems with ISO27000. *The TQM Journal*, 23(4), pp.367-376.
- Gjerdrum, D. and Peter, M., 2011. The new international standard on the practice of risk management—A comparison of ISO 31000: 2009 and the COSO ERM framework. *Risk management*, 31(2), pp.8-13.

- Goluch, G., Ekelhart, A., Fenz, S., Jakoubi, S., Tjoa, S. and Muck, T., 2008, January. Integration of an ontological information security concept in risk aware business process management. In *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual* (pp. 377-377). IEEE.
- Gordon, L.A., Loeb, M.P. and Tseng, C.Y., 2009. Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy*, 28(4), pp.301-327.
- Gritzalis, D., Iseppi, G., Mylonas, A. and Stavrou, V., 2018. Exiting the Risk Assessment Maze: A Meta-Survey. *ACM Computing Surveys (CSUR)*, 51(1), p.11.
- Gritzalis, D., Stavrou, V., Kandias, M. and Stergiopoulos, G., 2014, March. Insider threat: enhancing BPM through social media. In *New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on* (pp. 1-6). IEEE.
- Hair, J., F., Black, W., C., Babin, B., J. Anderson, R., E. and Tatham, R. L. (2010). *Multivariate Data Analysis : A Global Perspective*. (7th Edition). New Jersey: Pearson Prentice Hall Publication.
- Hair, J.F. and Jnr, B., 2009. BJ, & Anderson, RE (2010). *Multivariate data analysis: A global perspective*.
- Hong, K.S., Chi, Y.P., Chao, L.R. and Tang, J.H., 2003. An integrated system theory of information security management. *Information Management & Computer Security*, 11(5), pp.243-248.
- Hosseini, A., Greenwood, D., Smith, J.W. and Sommerville, I., 2012. The cloud adoption toolkit: supporting cloud adoption decisions in the enterprise. *Software: Practice and Experience*, 42(4), pp.447-465.
- Humphreys Edward, Plate Angelika. (2008) *ISMS risk management*. BSI Publications.
- Humphreys Edward. (2007) *Implementing the ISO/IEC 27001 information security management system standard*. Artech Press.
- Humphreys, E., (2008) *Information security management standards: Compliance, governance and risk management*. *Information security technical report*, 13(4), pp.247-255.

- Information Security Forum (ISF) (1997). Simplified practical risk analysis methodology (SPRINT) user guide. p. 43–57. URL http://www.citicus.com/report_esf_sprint.asp Information security risk management.
- International, H. (2019). *Health Level Seven International - Homepage | HL7 International*. [online] HL7.org. Available at: <http://www.hl7.org/> [Accessed 11 Jul. 2019].
- Internet world stats, 2017 Accessed on 7 April 2017 URL <http://www.internetworldstats.com/stats.htm>
- ISO. BS ISO 31000:2009. 2009 Risk management. Principles and guidelines.
- ISO. BS ISO/IEC 27005:2011. 2011 Information technology. Security techniques.
- Jensen, M.B., Philipsen, M.P., Møgelmoose, A., Moeslund, T.B. and Trivedi, M.M., 2016. Vision for looking at traffic lights: Issues, survey, and perspectives. *IEEE Transactions on Intelligent Transportation Systems*, 17(7), pp.1800-1815.
- Jin, Z. and Chen, Y., 2015. Telemedicine in the cloud era: Prospects and challenges. *IEEE Pervasive Computing*, 14(1), pp.54-61.
- Joseph, R. and Brown, P., 2017. The Cloud Gets Personal: Perspectives on Cloud Computing for Personalized Medicine. *International Journal of E-Health and Medical Communications (IJEHMC)*, 8(2), pp.1-17.
- Joshi, A., Kale, S., Chandel, S. and Pal, D.K., 2015. Likert scale: Explored and explained. *British Journal of Applied Science & Technology*, 7(4), p.396.
- Karabacak, B. and Sogukpinar, I., 2005. ISRAM: information security risk analysis method. *Computers & Security*, 24(2), pp.147-159.
- Kazemi, M., Khajouei, H. and Nasrabadi, H. (2012). Evaluation of Information Security Management System Success Factors: A Case Study of Municipal Organisation. *African Journal of Business Management* Vol. 6(14), pp. 4982-4989.
- Khajeh-Hosseini, A., Sommerville, I., & Sriram, I. (2010). Research challenges for enterprise cloud computing. arXiv preprint arXiv:1001.3257.
- Khajeh-Hosseini. (2013). Supporting system deployment decisions in public cloud, A thesis submitted for the degree of PhD at the University of St Andrews.
- Kifor, T., Varga, L. Z., Vazquez-Salseda, S., Alvarez, S., Willmott, S., Miles, S., & Moreau, L. (2006). Provenance in Agent-mediated Healthcare Systems. *Intelligent Systems*, IEEE , 21(6), 38-46. DOI: 10.1109/MIS.2006.119.

- Kingston Hospital NHS Foundation Trust. 2017. URL <https://www.kingstonhospital.nhs.uk/media/202487/enc-m-corporate-risk-register-at-18-01-16.pdf>
- Labunets, K., Massacci, F. and Paci, F., 2013, October. An experimental comparison of two risk-based security methods. In *Empirical Software Engineering and Measurement, 2013 ACM/IEEE International Symposium on* (pp. 163-172). IEEE.
- Labunets, K., Paci, F., Massacci, F. and Ruprai, R., 2014, August. An experiment on comparing textual vs. visual industrial methods for security risk assessment. In *Empirical Requirements Engineering (EmpiRE), 2014 IEEE Fourth International Workshop on* (pp. 28-35). IEEE.
- Lalonde, C. and Boiral, O., 2012. Managing risks through ISO 31000: A critical analysis. *Risk management*, 14(4), pp.272-300.
- Lam, H.Y., Choy, K.L., Ho, G.T.S., Cheng, S.W. and Lee, C.K.M., 2015. A knowledge-based logistics operations planning system for mitigating risk in warehouse order fulfilment. *International Journal of Production Economics*, 170, pp.763-779.
- Latif, R., Abbas, H., Assar, S., & Ali, Q. (2014). Cloud computing risk assessment: a systematic literature review. In *Future Information Technology* (pp. 285-295). Springer Berlin Heidelberg.
- Li, G., Xu, B., He, R.X. and Zhang, S.X., 2017. Using Healthcare Failure Mode and Effect Analysis to Reduce Intravenous Chemotherapy Errors in Chinese Hospitalised Patients. *Cancer nursing*, 40(2), pp.88-93.
- Li, M., Yu, S., Ren, K. and Lou, W., 2010, September. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In *International Conference on Security and Privacy in Communication Systems* (pp. 89-106). Springer Berlin Heidelberg.
- Lian, J. W., Yen, D. C., & Wang, Y. T. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. *International Journal of Information Management*, 34(1), 28-36.
- Liang, Y., Qi, G., Wei, K. and Chen, J., 2017. Exploring the determinant and influence mechanism of e-Government cloud adoption in government agencies in China. *Government Information Quarterly*.
- Lisiak-Felicka, D. and Szmit, M., 2014. Information security management systems in Marshal Offices in Poland. *Information Systems In Management*, 3(2), pp.134-144.

- Liu, W., & Park, E. K. (2013). e-Health care Cloud-Enabling Characteristics, Challenges and Adaptation Solutions. *Journal of Communications*, 8(10), 612-619.
- Lubamba, C. and Bagula, A., 2017, July. Cyber-healthcare cloud computing interoperability using the HL7-CDA standard. In *Computers and Communications (ISCC), 2017 IEEE Symposium on* (pp. 105-110). IEEE.
- Lupse, Oana-Sorina & Mihaela, Marcella & Vida, Lăcrămioara & Stoicu-Tivadar, Vasile. (2018). *Cloud Computing and Interoperability in Healthcare Information Systems*.
- M. Dlamini, J. Elo, M. Elo, (2009) "Information security: The moving target," *Computers and Security*, vol. 28, iss. 3-4, pp. 189-198.
- Mahy, Y., Ouzzif, M. and Bouragba, K., 2016. Toward a shared view of IT governance. *International Journal of Innovation, Management and Technology*, 7(4), p.125.
- Mansfield, J.G., Caplan, R.A., Campos, J.S., Dreis, D.F. and Furman, C., 2015. Using a quantitative risk register to promote learning from a patient safety reporting system. *The Joint Commission Journal on Quality and Patient Safety*, 41(2), pp.76-AP1.
- Mao, M. and Humphrey, M., 2014. Resource Provisioning in the Cloud: An Exploration of Challenges and Research Trends. In *Handbook of Research on Architectural Trends in Service-Driven Computing* (pp. 589-612). IGI Global.
- Martin-Flatin, J.P., 2014. Challenges in cloud management. *IEEE Cloud Computing*, 1(1), pp.66-70.
- Masrom, M. and Rahimli A,A. (2014) Review of Cloud Computing Technology Solution for Healthcare System . *Research Journal of Applied Sciences, Engineering and Technology* 8(20).
- Masrom, M. and Rahimli, A., 2015. Cloud Computing Adoption in the Healthcare Sector: A SWOT Analysis. *Asian Social Science*, 11(10), p.12.
- Mayer, N., Barafort, B., Picard, M. and Cortina, S., 2015, September. An ISO compliant and integrated model for IT GRC (Governance, Risk Management and Compliance). In *European Conference on Software Process Improvement* (pp. 87-99). Springer, Cham.
- Ministry of Health in Oman (2017) URL: <https://www.moh.gov.om/en/web/directorate-general-of-information-technology/future-projects>. [Accessed on 11-04-2017] .

- Moody, D.L., 2003. The method evaluation model: a theoretical model for validating information systems design methods. *ECIS 2003 proceedings*, p.79.
- Mxoli, A., Gerber, M., & Mostert-Phipps, N. (2014, November). Information security risk measures for Cloud-based personal health records. In Information Society (i-Society), 2014 International Conference on (pp. 187-193). IEEE.
- Năstase, P., Năstase, F. and Ionescu, C., 2009. Challenges generated by the implementation of the IT standards CobiT 4.1, ITIL v3 and ISO/IEC 27002 in enterprises. *Economic computation & economic cybernetics studies & research*, 43(1), p.16.
- National Centre for Statistics & Information (2017) Population Clock, Accessed on 10th April, 2017 Source: <https://www.ncsi.gov.om/Pages/NCSI.aspx> . [Accessed on 25-5-2015].
- Neuman, D., Neuman, M. and Kandaswamy, B., Isonetic Inc, 2018. *Dark virtual private networks and secure services*. U.S. Patent Application 15/789,909.
- New Horizon. Computer learning centre (2018) *COBIT vs ITIL Available at <https://blog.nhlearningsolutions.com/blog/tabid/145/artmid/16483/articleid/1514/cobit-vs-til>* [Accessed on 2 July, 2018].
- Oman Data Park (ODP), 2019 website <https://www.omandatapark.com/> [Accessed June 2019].
- Olsson, R., 2007. In search of opportunity management: Is the risk management process enough?. *International journal of project management*, 25(8), pp.745-752.
- Oxley, Catriona. 2015. Risk Assessment Procedure and Risk Register Guidance. NHS SHETLAND DOCUMENT.
- Patterson, F.D. and Neailey, K., 2002. A risk register database system to aid the management of project risk. *International Journal of Project Management*, 20(5), pp.365-374.
- Pipkin, D.L., 2000. *Information security: protecting the global enterprise*. Prentice Hall PTR.
- Quality One. 2017. *"FMEA / Failure Mode and Effects Analysis / Quality-One"*. quality-one.com. [Accessed 28-7-2017].

- Quality-One International Discover the value (2015) <http://quality-one.com/fmea/> [Accessed 10 August 2017].
- Rahman, N. H. A., & Choo, K. K. R. (2015). Factors Influencing the Adoption of Cloud Incident Handling Strategy: A Preliminary Study in Malaysia. In Proceedings of 21st Americas Conference on Information Systems, AMCIS 2015, *arXiv preprint arXiv:1505.02908*. <http://aisel.aisnet.org/amcis2015/ISSecurity/GeneralPresentations/17/> .
- Rasid, A., Zaleha, S., Golshan, N., Mokhber, M., Tan, G.G. and Mohd-Zamil, N.A., 2017. Enterprise Risk Management, Performance Measurement Systems and Organizational Performance in Malaysian Public Listed Firms. *International Journal of Business & Society*, 18(2).
- Recker, J.C. and Rosemann, M., 2010. A measurement instrument for process modeling research: development, test and procedural model. *Scandinavian Journal of Information Systems*, 22(2), pp.3-30.
- Reid, R.C. and Floyd, S.A (2001), "Extending the risk analysis model to include market insurance", *Computers & Security*, Vol.20 No 4, pp331-9.
- Ren, L., Zhang, L., Wang, L., Tao, F. and Chai, X., 2017. Cloud manufacturing: key characteristics and applications. *International Journal of Computer Integrated Manufacturing*, 30(6), pp.501-515.
- Riskworld.net. (2017). COBRA - Security Risk Assessment, Security Risk Analysis and ISO 17799 / BS7799. [online] Available at: <http://www.riskworld.net/> [Accessed 1 May 2017].
- Rodríguez, A., Fernández-Medina, E. and Piattini, M., 2007. A BPMN extension for the modeling of security requirements in business processes. *IEICE transactions on information and systems*, 90(4), pp.745-752.
- Rosemann, M. and vom Brocke, J., 2015. The six core elements of business process management. In *Handbook on business process management 1* (pp. 105-122). Springer Berlin Heidelberg.
- Rösler, P., Mainka, C. and Schwenk, J., 2018. More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema.
- Rottermann, C., Kieseberg, P., Huber, M., Schmiedecker, M. and Schrittwieser, S., 2015, December. Privacy and data protection in smartphone messengers. In Proceedings of the 17th International Conference on Information Integration and Web-based Applications & Services (p. 83). ACM.

- Rukh, L. and Malik, A.A., 2017, April. Swiss army knife of software processes generic framework of ISO 27001 and its mapping on resource management. In *Communication Technologies (ComTech), 2017 International Conference on* (pp. 12-15). IEEE.
- Salnitri, M., Dalpiaz, F. and Giorgini, P., 2014. Modeling and verifying security policies in business processes. In *Enterprise, Business-Process and Information Systems Modeling* (pp. 200-214). Springer, Berlin, Heidelberg.
- Sahi, M.A., Abbas, H., Saleem, K., Yang, X., Derhab, A., Orgun, M.A., Iqbal, W., Rashid, I. and Yaseen, A., 2018. Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions. *Ieee Access*, 6, pp.464-478.
- Salnitri, M., Dalpiaz, F. and Giorgini, P., 2017. Designing secure business processes with SecBPMN. *Software & Systems Modeling*, 16(3), pp.737-757.
- Sekgwaleo, T., 2018. Understanding Traditional Systems Development Methodologies. *IJAME*.
- Shaojie, W.A.N.G., Liang, H.O.U., Lee, J. and Xiangjian, B.U., 2017. Evaluating wheel loader operating conditions based on radar chart. *Automation in Construction*, 84, pp.42-49.
- Sharma, S.K., Al-Badi, A.H., Govindaluri, S.M. and Al-Kharusi, M.H., 2016. Predicting motivators of cloud computing adoption: A developing country perspective. *Computers in Human Behavior*, 62, pp.61-69.
- Sherwood, J., Clark, A., Lynas, D., 2005 *Enterprise Security Architecture: A Business-Driven Approach*. CMP Books.
- Shini.S.G, Dr.Tony Thomas, Chithraranjan.K (2012) Cloud Based Medical Image Exchange-Security Challenges, *Procedia Engineering* 38, SciVerse ScienceDirect 3454-3461.
- Shoemaker, D., Bawol, J., Drommi, A., 2004. A Delivery Model for an Information Security Curriculum. In *Proceedings of the Third Security Conference*, (Las Vegas, Nevada, USA), Information Institute, 2004.
- Shostack (2012) "The evolution of information security" in *The Next Wave: Developing a blueprint for a science of cybersecurity*, vol. 19(2).
- Shostack, A., 2014. *Threat modeling: Designing for security*. John Wiley & Sons.

- Singh, Narain A., Gupta, M.P. and Ojha, A., 2014. Identifying factors of “organizational information security management”. *Journal of Enterprise Information Management*, 27(5), pp.644-667.
- Skilton, A. (2011) *Supporting the Information Systems Requirements of Distributed Healthcare Teams*. PhD Thesis. Cardiff University.
- Spikin, I.C., 2013. Risk Management theory: the integrated perspective and its application in the public sector. *Estado, Gobierno y Gestión Pública*, (21), pp.pp-89.
- Spink, J., Moyer, D.C. and Speier-Pero, C., 2016. Introducing the food fraud initial screening model (FFIS). *Food Control*, 69, pp.306-314.
- Stavrou, V., Kandias, M., Karoulas, G. and Gritzalis, D., 2014, September. Business Process Modeling for Insider threat monitoring and handling. In *International Conference on Trust, Privacy and Security in Digital Business* (pp. 119-131). Springer International Publishing.
- Stolen, K., den Braber, F., Dimitrakos, T., Fredriksen, R., Gran, B.A., Houmb, S.H., Lund, M.S., Stamatiou, Y. and Aagedal, J.O., 2002. Model-based risk assessment—the CORAS approach. In NIK (2002) informatics conference, Kongsberg.
- Subramaniam, N., Collier, P., Phang, M. and Burke, G., 2011. The effects of perceived business uncertainty, external consultants and risk management on organisational outcomes. *Journal of Accounting & Organizational Change*, 7(2), pp.132-157.
- Sultan, N., 2014. Making use of cloud computing for healthcare provision: Opportunities and challenges. *International Journal of Information Management*, 34(2), pp.177-184.
- Sultan, N., 2015. Reflective thoughts on the potential and challenges of wearable technology for healthcare provision and medical education. *International Journal of Information Management*, 35(5), pp.521-526.
- Susanto, H., Almunawar, M.N. and Tuan, Y.C., 2011. Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, 11(5), pp.23-29.
- Syalim, A., Hori, Y. and Sakurai, K., 2009, March. Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide. In *Availability, Reliability and Security, 2009. ARES'09. International Conference on* (pp. 726-731). IEEE.
- Shirazi, F., Seddighi, A. and Iqbal, A., 2017, July. Cloud Computing Security and Privacy: An Empirical Study. In *International Conference on Human-Computer Interaction* (pp. 534-549). Springer, Cham.

- Tabachnick, G. B. and Fidell, L. S. (2001) Using Multivariate Statistics. (4th Edition) U.S.A: Allyn and Bacon.
- Taylor, Joanne 2013. Concepts of Strategic Risk and management Strategic Risk. Presentation to the Strategic Planning Task Force.
- Teclaw, R., Price, M.C. and Osatuke, K., 2012. Demographic question placement: Effect on item response rates and means of a veterans health administration survey. *Journal of Business and Psychology*, 27(3), pp.281-290.
- The Broadband Commission for Digital Development , (2016) The State of Broad Band in 2015, Accessed on 8th February <http://www.broadbandcommission.org/documents/reports/bb-annualreport2015.pdf> .
- The knowledge Academy (2018). <https://www.theknowledgeacademy.com/blog/prince2-vs-agile/> [Accessed on July 2018].
- Tomanek, M. and Juricek, J., 2015. Project risk management model based on PRINCE2 and SCRUM frameworks. *arXiv preprint arXiv:1502.03595*.
- Tran, T.H.D., 2017. *Risk Assessment Based on CORAS and Fuzzy logic* (Master's thesis).
- Tudor, J.K. (2001) Information Security Architecture, CRC Press Boca Raton, FL. Not in ch 2
- Uta, L., Chiliya, N., & Chuchu, T. (2014). Determining the Feasibility of Adopting Technological Innovation to Enhance Service Delivery in Selected Johannesburg Health Institutions. *Mediterranean Journal of Social Sciences*, 5(25), 148.
- Van Haren Publishing. (2018) ISO/IEC 38500 for IT Governance URL: <https://www.vanharen.net/blog/it-management/isoiec-38500-for-it-governance-in-3-minutes/> [Accessed on 09.07.2018].
- Venter, H.S. and Eloff, J.H., 2003. A taxonomy for information security technologies. *Computers & Security*, 22(4), pp.299-307.
- Vincent, D.W. and Honeck, W., 2004. Risk Management analysis techniques for validation programs. *Journal of validation technology*, 10, pp.235-251.

- Vorster, A. and Labuschagne, L.E.S., 2005, July. A framework for comparing different information security risk analysis methodologies. In *Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries* (pp. 95-103). South African Institute for Computer Scientists and Information Technologists.
- Vilarinho, S. and da Silva, M.M., 2011, October. Risk management model in ITIL. In *International conference on ENTERprise information systems* (pp. 306-314). Springer, Berlin, Heidelberg.
- Ward S. (1999) Assessing and managing important risks. *International Journal of Project Management*;17:331–6.
- Wendy L. Currie, Jonathan J. M. Seddon. A Cross-Country Study of Cloud Computing Policy and regulation in Healthcare. In *Proceedings of 22st European Conference on Information Systems, ECIS 2014*.
- Whitman, M. and Mattord, H. (2012) *Principles of Information Security*, 4th edition, Course Technology, Cengage Learning.
- Wijaya, A.A., Purnama, J., Soetomo, M.A.A. and Eng, K.I., 2014, September. Indonesian awareness of health record stored in cloud computing. In *ICT For Smart Society (ICISS), 2014 International Conference on* (pp. 77-81). IEEE
- Williams TM. (1993) Risk-management infrastructures. *International Journal of Project Management* ;11:5–10.
- Woody, C., Coleman, J., Fancher, M., Myers, C. and Young, L., 2006. *Applying octave: Practitioners report* (No. CMU/SEI-2006-TN-010). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.
- World Health Organization, 2017. Strengthening national capacity for patient and community engagement and empowerment in health care in Oman:(No. WHO/HIS/SDS/2017.2). World Health Organization. Regional Office for the Eastern Mediterranean.
- Wright, M. (1999), “Third generation risk management practices”, *computers & Security*, Vol. 1999 No.2, pp. 9-12.
- Xu, B., Xu, L., Cai, H., Jiang, L., Luo, Y. and Gu, Y., 2017. The design of an m-Health monitoring system based on a cloud computing platform. *Enterprise Information Systems*, 11(1), pp.17-36.

- Xu, K., Attfield, S., Jankun-Kelly, T.J., Wheat, A., Nguyen, P.H. and Selvaraj, N., 2015. Analytic provenance for sensemaking: A research agenda. *IEEE Computer Graphics and Applications*, 35(3), pp.56-64.
- Yazar, Z., 2002. A qualitative risk analysis and management tool–CRAMM. SANS InfoSec Reading Room White Paper.
- Yeandle, J., Gordon, C., Challis, E. and Fawkes, L., 2013. Risk assessment and management of people with personality disorders: Jane Yeandle and colleagues outline an approach staff can use to address harmful behaviour that focuses on the patient's relationships. *Mental Health Practice*, 17(2), pp.21-23.
- Youssef, A.E., 2014. A framework for secure healthcare systems based on big data analytics in mobile cloud computing environments. *Int J Ambient Syst Appl*, 2(2), pp.1-11.
- Zhang, Y., Qiu, M., Tsai, C.W., Hassan, M.M. and Alamri, A., 2017. Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. *IEEE Systems Journal*, 11(1), pp.88-95.

10 Appendixes

11 Appendix A: Interview Questions

A.1: Interview Questions to Managers to Migrate Healthcare Services to Cloud

Meeting main

To understand manager's and healthcare providers attitude towards migrating healthcare services to cloud computing. It considers migrating process from management, technical, legal and security prospective. In addition, it focusses on cloud security checklist any healthcare provider would like to consider before migrating their healthcare services to cloud.

Meeting Questions

Category	Question list
Role in the organization	1. What are the roles you play in the healthcare organization(s)? Give more details about each role.
Management perspective	2.What do you think about migrating healthcare service to cloud? 3. Would system administrators be happy to give up some of their control over systems and rely on cloud service providers for the support of end users? 4.How would departments react to the migration of applications and data to cloud service providers? They might not have the same level of access to a cloud as they currently do to their internal systems, so how would they have to change their working practices?
Security (Data storage, process and transfer)	5.What do you think the role of security is/ should be in healthcare? 6.What is the backup plan for data stored in the cloud? 7. Will the data be encrypted in the cloud? How will it processed or transferred? 8.Will the data be isolated ? 9.Can the data be portable to different cloud provider? How long it will take to migrate to another cloud? Is there a special tool for exporting data? 10.Does your cloud service provide data integrity and availability? 11.How the original data be deleted ? Is it actually erased when contract terminated. 12. Is it monitored? From provider to ensure acceptable use and customer

	Can the data be Non-repudiation?
Security (Access control)	<p>13.Does your cloud provider provide management access control within healthcare?</p> <p>14.does your cloud provider have “backdoor” for maintenance, support and services</p> <p>User/patient access control in the healthcare</p>
Security (procedure)	<p>15.Does your cloud provider provide “Auditing”</p> <p>Certification (customer to check is it relevant to their work or not) and does it follow Personal Identifiable Information(PII) ISO/IEC 27018:2014</p> <p>16.Countermeasures- how does your cloud provider react about security breach?</p> <p>17.Testing (cloud provider what kind of security tests)</p> <p>18.If there is breach of security will the provider provide a notification to customers or not? Detection Key management Security level</p>
Incident management	<p>18.How security incident are dealt with? Does cloud provider provide: Response? Logging? Reporting? Forensics?</p> <p>19.Is there a certain mechanism to notify customers about data breaches or information security incident?</p>
Privacy	<p>20.Non-disclosure? Can provider use or access the data?</p> <p>Data minimization</p>
Hybird clouds	<p>21. Does your cloud provide rely on outsourcing some of the services? (may rely on the services from multiple provider)</p>
Technical	<p>22. Does your cloud provider face or likely to some of the following technical issues? if yes, how it deals with? Resource exhaustion (under or over provisioning) Isolation failure Cloud provider malicious insider- abuse of high privilege roles Management interface compromise (manipulation, availability of infrastructure) Intercepting data in transit Insecure or ineffective deletion of data Distributed denial of service (DDoS) Economic denial of service (EDoS) Loss of Cryptographic Keys Compromise service engine Conflicts between customer hardening procedures and cloud environment</p>

Legal	<p>23. Does your cloud provider clarify the status of the legal issues for instance: Risk from changes of jurisdiction Data protection risks Licensing risks</p> <p>24. Does your cloud provider follow Health Insurance Portability and Accountability Act (HIPAA)?</p> <p>25. Does your cloud provider follow Personal Information Protection and Electronic Documents Act (PIPEDA)?</p>
Risks not specific to the cloud	<p>26. Does your cloud provider face or likely to some of the following issues? Network breaks Network management (network congestion/mis-connection/non-optimal use) Modifying network traffic Privilege escalation Social engineering attacks (impersonation) Loss or compromise of operational logs Loss or compromise of security logs (manipulation of forensic investigation) Backups lost, stolen Non Cloud-Specific Network-Related Technical Failures or Attacks Natural disasters</p>
Further recommendation	<p>27. Do you recommend anyone who we can speak to about the areas we mentioned above? (For example, those dealing with Information Governance, Information systems, or cloud provider)</p>

A.2 Glossary Terms for Interview Questions

Cloud computing from e-Healthcare: an application- oriented and services-based infrastructure where Health-IT resources are pooled, allowing services to be widely deployed or rapidly shared in response to changing healthcare business and regulatory requirements. (e.g., networks, servers, storage, applications, and services).

Security

Data Encrypted: Convert (information or data) into a code, especially to prevent unauthorized access.

Data Isolated: Data not accessible to others

Data Portable: data can be moved from one cloud to another

Data integrity: refers to the accuracy and consistency of data stored in a database.

Cloud monitoring: It is the process of reviewing, monitoring and managing the operational workflow and processes within a cloud-based IT asset or infrastructure to ensure that a cloud infrastructure or platform performs optimally.

Non-repudiation: is a method of guaranteeing data transmission between parties via digital signature and/or encryption. It is one of the five pillars of information assurance (IA). The other four are availability, integrity, confidentiality and authentication. It is mainly used for digital contracts, signatures and email messages.

Auditing: accredited auditors may perform independent audit of cloud providers and their datacenters.

Countermeasures: It is an action, process or device or system can prevent or mitigate the effects of threats to server or networks.

Forensics: Cloud forensics is the application of digital forensics in cloud computing as a subset of network forensics. It is a cross-discipline between cloud computing and digital forensics

Non-disclosure: it is a signed formal agreement between two parties where the first party agree to give the second party confidential information about product. The second party agree not to share this information with anyone else for a certain period.

Outsourcing some of the services: obtain more than one cloud provider for various services

Technical

Resource exhaustion As Cloud services are on-demand services, there is the possibility that the CP will not be able to 1) meet an increased demand in a certain shared resource, or 2) to maintain a given service level.

Isolation failure: In shared environments, errors or attacks can lead to situations where one tenant has access to another tenant's resources or data. In the case of attacks, an attacker gets access to the resources or data of a specific customer, or even of all customers of the Cloud service. Thus, it covers the failure of mechanisms separating storage, memory, routing and reputation between different tenants.

Cloud provider malicious insider: Abuse of high privilege roles (i.e examples include CP system administrators and managed security service providers).

Management interface compromise (manipulation, availability of infrastructure) the customer management interfaces of public cloud providers are Internet accessible and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk especially when combined with remote access and web browser vulnerabilities.

Intercepting data in transit

Whenever data is transferred between different computers or sites, there is the possibility that the transfer can be intercepted, this is especially relevant in shared environments and when data is transferred between sites (e.g. between CC and CP).

Insecure or ineffective deletion of data:

Deleting data from Cloud storage does not in fact mean that the data is removed from the storage or eventual backup media. If disk storage is not encrypted, the data could be accessed at later time by another customer of a Cloud provider.

Distributed denial of service (DDoS): Distributed Denial of Service attacks aim at overloading a resource (network or service interface) by flooding it with requests from many sources distributed across a wide geographical or topological area, so that the legitimate users are unable to use the resource as intended..

Economic denial of service (EDOS): As a consequence of attacks, poor budget planning, or misconfigurations, the cost of a Cloud service can strain the financial resources of a CC to an extent that the service is no longer affordable.

Loss of Cryptographic Keys:

The loss or compromise of cryptographic keys used for encryption, authentication or digital signatures can lead to data loss, denial of services, or financial damages

Compromise service engine: A compromise of the service engine will give an attacker access to the data of all customers, resulting in a potential complete loss of data or denial of service.

Conflicts between customer hardening procedures and cloud environment

Certain security measures of a Cloud Customer may conflict with a Cloud Providers environment, making their implementation by the Cloud Customer impossible.

Legal

Risk from changes of jurisdiction

When data is stored or processed in a data centre located in a country other than the CC's, there are numerous ways in which the change in jurisdiction could affect the security of the information. Examples include: 1) Data might be seized or the operations of a service disrupted due to reasons that don't exist in the CC's country. 2) In some cases, national security interests of the hosting country might be cited as a reason for seizing data. 3) Additionally, a CP might be subject to law enforcement or national security actions from the

country its business headquarters is based in, not just those from the countries where its data centers are located.

Data protection risks

Processing data in another country may incur difficulties regarding data protection legislation, or might even be considered unlawful by the responsible Data Protection authority.

Licensing risks

Violating a software supplier's licensing agreements can result in significant financial penalties or disruptions of service.

Risks not specific to the cloud

Privilege escalation: it is the act of abusing a bug or design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

Social engineering attacks: Social engineering is understood to mean the art of manipulating people into performing actions or divulging confidential information. While it is similar to a confidence trick or simple fraud, it is typically trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victims.

Backups lost, stolen: The backups a CP makes of its customers' data can get lost, damaged, or the physical media on which the backup is stored can get stolen.

Non Cloud-Specific Network-Related Technical Failures or Attacks:

Cloud services can be affected by a number of network-related technical failures that can also occur on classic IT settings. Examples include the loss of Internet connectivity due to failures at the CC's site or the CC's Internet service provider, temporarily reduced network bandwidth on the path between CC and CP, disruptions in the global Internet routing infrastructure leading to the loss of the network path between CC and CP, and failures of the CP's Internet connectivity.

Natural disasters: Natural disasters like flooding and earthquakes can affect the infrastructure of a Cloud Provider. This way, a Cloud Customer might be affected by natural disasters occurring far away from its own location.

A.3 Interview Transcript with CC01

Interview transcript No 1

Date: 18th Sep, 2015

Voice file name: Meeting with CC01

Duration: 0.17mins

Typist comments regarding dictation: Mostly clear

VOICE FILE NAME: Meeting with CC01 (16 June, 2015)

Key:

I = Interviewer Woman

R = Respondent

Aah = sounds like

I Good morning CC01 can you please introduce your name and your role in the organisation?

R Aah.. my name CC01 and I'm professor in the department of genetics..aah I'm an academician but also involved in healthcare as person in charge as diagnostics for genetics disease.

I Aah.. basically my research is about migrating healthcare services to cloud computing what do think about this idea?

R Ah.. its fantastic idea and something that we will be moving to it in any way. We can't avoid it technology is improving at high speed and we are already moving to it in other fields and areas. And healthcare is also already moving to it. There is so many problems we can resolve using IT.

I Do you think that system administration will be happy giving their role and control to cloud provider rather than have it indoor?

R Definitely, if they understand that this is all confidential and this is all user name and password based. They will definitely welcome the idea. Especially that the system that they are using now. In terms of Health care and family history and things like that. It all also same way that it computerized and highly sophisticated. And something that resolves problems related to security and confidentiality that we have at the moment. Moving to cloud may resolve these issues.

I What about the department? Will the staff be looking forward to this movement or it will be or reluctant?

R Aah based on my short experience. So your questions is based on our environment here not in Oman in general in Sultan Qaboos University

Hospital. Based on my experience.. There is always be people who will be against the idea especially when it comes to security and confidentiality, facilities things like that. Obviously, the idea is new and it has to be brain stormed ..ahh... by inclusion of all concerned people; administration, scholars, scientist, physicians and people from the public the community. So all these people have to brain stormed the idea before it can be applied you know .. so that everybody is happy and gives the green light.. but I can tell you that everyone will welcome the idea. But the application of it .. there will be some problems.. that's why all these people and the parties that were concerned have to be involved in brain storming and discussing the idea.

I Alright.. in terms of security what do you think of having a backup of the systems of the cloud.

R Aah okay so there are two securities here. The first one is obviously when you have data.. you are worried you gona lose it because of disaster or natural disaster and things like that aahh so you must have a backup.it is like your phone you must have backup. That back up will have also security and confidentiality who will have access to that backup? Because you are duplicating here.. as soon as duplication of original .. its like you are holding confidential dossier that dossier as soon as you duplicate it you are increasing the level of security and you are increasing the error . human error. So obviously yes there should be backup and you must secure the backup.

I Sometimes they encrypt the data before putting it in the cloud. What do you think of that ?

R They do what?

I Encryption? Means they verify the data into codes then they store it in the cloud.

R Ahha .. they code the data aah will that have some .. hum let say there are error problems and you lose the coding something like that how would you bring back your data ?

I This is one of the risks from IT prospective

R So I think highly knowledge people in the field should be consulted.

I Do you think the data can be portable to different cloud provider in case one cloud provider will have some issues in it ? and then is it necessary in the agreement itself to know that data is portable to another cloud provider or not?

R What do you mean about cloud provider from one country to another or do mean it just different companies.

I Yes different companies

R I think it should be possible through agreement.. Signed consents and agreements so if there is any breach ..aah.... the company will be responsible.

I Sometimes the company would like to monitor the data in the cloud. Is that acceptable from healthcare perspective?

- R If it is coded yes. If there is no name of the patient that's fine. For example do not mention my name but as in A B C D . yes you can but again there is another risk. I will give you an example. You know as an Academic who does mainly a research. Sometimes for us when we have a project. We want for example study a disease what we do we have access to the system. We can access the system and collect all the clinical data of the patient. There are companies now that sell the data. A real data. Even if I put A on the patient. At least I know it has this age this clinical data. What I am concerned about is the disease and clinical features. I'm not concerned about the name of the patient my mainly concern is the disease we are studying. There are companies who sell a real data to investigators. They will sell it to me without you know.so if you allow the company to the data they may sell without uou know selling it worldwide. So there should be some agreement as well.
- I **What about management access control? Do you think that patient should have access to his own data?**
- R Yes I think so .
- I **So basically patient owns the data not like let say Sultan Qaboos University?**
- R Yes based on patient user name and password should be the only one who has access as I said before and his own physician.. but even the physician should sign the consent form.
- I **I'm asking because some hospitals consider the health information belongs to the hospital not the patient.**
- R No it is the patient life not them.. any body in the hospital they finish their shift they go home right but the patient who would like to know what's going on. Not only that the hospital is responsible for any change to the data. As soon as the patient undergoes a surgery or treatment. He has to know what has been going through what are the consequences what is treatment has been giving. As you can see now in the west when go to a physician to do surgery you have the right to ask all questions they will explain to you in details what's going to happen and then what are the consequences. Then you have to sign on consent on those consequences. They will tell you look you have 20% to live and 80% probability to die and you get consent for that. So hospital does not own anything. The only thing the hospital can do is interfering and give the consultation to the patient.
- I **As I know in UK for example the health data belongs to the hospital or GP not to the patient . It was kind of strange.**
- R The physician has gone through a training for 7 or 8 years. During those years there is a course of bioethics. How to break a bad news to a patient. Obviously yes. If I'm a doctor for me to tell you .. that you have cancer . obviously I'm the first to have access to this information right but it is not my information right it is your information it concerns you first. so first of all I have to break the news to you and the family. Second I do not own that information. As soon as I break the news. You own the information and I have no right to tell any body without your consent. So all in all you are the owner.

- I** What about you know ..the cloud provider ..aah.. basically these are technical terms I won't go through it as it not really related your area.. ah..but let say in case of networks breaks.. you do not have access to the internet ..and the patient information is stored in the cloud.. how would you think and react about it. As physician ?
- R** Aah .. see that's why there should always be a backup. Now why are we moving to cloud? To avoid the paper work right. The hassle of paper work and store data and things like that right. It would be nice once the network is off I have an access somehow. And the only way I can either on file. I can pull the patient file from hospital but we do not want that. We want hospital that do not have storage no files. Everything is computerized. Now that's why IT people has to think of having a backup somewhere. Like electricity when there is break out of electricity what do we have we have emergency plugs. For example during a storm, we know electricity will cut off. In our genetics department we store sample data in fridge. Those fridges has red plugs that turn on automatically for few hours to save the sample. Especially if we have sample blood from a patient who passed away. Then there is no way to have the sample blood again.
- I** Yeah .. right.. finally Do you recommend anyone who we can speak to about the areas we mentioned above?
- R** Yes you should meet someone from CIS department in SQU and someone from hospital administration to get a clear picture.
- I** Thank you so much.

A.4 Interview Transcript with CC02

Interview transcript no 2

Date: 19th Sep, 2015

Voice file name: Meeting with CC02

Duration: 0.17mins

Typist comments regarding dictation: Mostly clear

VOICE FILE NAME: Meeting with CC02. (21 June, 2015)

Key:

I = Interviewer Woman

R = Respondent

aah = sounds like

I Good morning Dr. CC02. my name is Aseela Al Harthi. I'm doing a research about migrating healthcare services to cloud computing. Can you please introduce yourself and your role in the organisation?

R yeah, I'm CC02. Associate professor in the department of Behavioral Medicine in Sultan Qaboos University. Specialist in child and adult Psychiatric.

I **Dr. my research will be mainly about migrating healthcare services of patients and medical service to cloud computing. Which means it will available at any time any where.through the internet. Do you support this idea?**

R yeah, I support it provided that the security for the patient's secrets and states should kept confidential. But it is good idea to communicate with other colleagues in other hospitals and other countries. To exchange idea and opinion about certain conditions and cases.

I **some will argue that medical information belongs to the hospital not the patient what do you think about it?**

R well really it is okay it is related to HIS or IT system but the secrets of the patients is as well should be considered in secret way and appropriate way. Because the confidentiality is crucial issue to consider. Patient care is different from other cases. Some people do not like for others to know their condition or their diagnosis of certain disease because of social stigma or something like that as it can affect their work and social states in the community. So this should be considered crucial actually.

I **let us assume the confidentiality of the patient information is there and the security is the data is guaranteed somehow. What about the attitude of the medical staff? Will they support migrating their role to the cloud rather than physical work in the hospital. For example register as new patient or book an appointment.**

R I think they will support it because it is for the future is a necessity. Because science and communication is advancing very fast. And we do need to transmit our information of certain cases with other colleagues. So to have such assistance it will facilitate the

communication process with others and reduce the time and effort now taking by putting or writing special medical reports. And to be transferred to our colleagues in another hospital for follow up or diagnosis or treatment of some cases. So this will actually have a great advantages for both sides doctors and patients.

I okay, what in terms of emergency let say there are networks breaks. What alternative way to deal with the patients data?

R There should be a plan from IT department or from HIS that can deal with such disasters and crises when they happen actually in order to prevent any problem or any delay in the delivery of the service or treatment of the patient and to avoid any complication that might happen in this concern. Actually this is a technical problem that should be dealt properly with specialised people in the IT and information technology systems.

I alright let say from the medical side, you as a doctor do you prefer to see all your patient data available online at any time? Let say you are travelling abroad and there some case that need your opinion. In that case. Will support having this data online so you can access via username and password? In order to give your diagnose or input what to do next?

R Yes I supported it provided again the confidently will be available and secure in all steps. But if the confidently will be lost then the confidence of the patients on us and the system will be disturbed very much.

I In normal cases is there like a recovery plan for patient data as it is right now? Is it stored in the hospital?

R Up to my knowledge yeah it is stored in the hospital in HIS systems. All the information are there actually.

I according to the recent events in Oman. There were many natural disaster like Guno in 2007 then Feet in 2008 and recently Ashwaya in 2015. So does it affect the information stored in the hospital in any way?

R Yeah Of Course, if we do not be prepared to deal with such crises and problems encounter in such events. Then all information will be lost and this will be a real tragedy. The technical people should think about these problems and should keep the data in save place in addition to kept it available in the system itself. In a separate place away from the hospital. For instance in ministry of health or somewhere else in order to use the extra data when the original data be lost or destroyed by floods or by some other disasters.

I Finally I would like to ask for your opinion. Do you recommend a certain Doctor or a person to meet regarding the same topic. Information systems or medical side?

R Well. You can select any doctor work in the hospital they are very cooperative if they have time as you know time is very important. Maybe Dr. Samir Al Adawi might be available. You can check his timing with his coordinator Ms. Ruqayah.

I What is his title?

R Prof. Samir Al Adawi is professor and head of behavioural medicine department.

I Alright. Thank you so much for your time I really appreciate it.

A.5 Interview Transcript with CC03

Interview transcript no 3

Date: 19th Sep, 2015

Voice file name: Meeting with CC03 , Manager for Cloud Initiatives, Information Technology Authority

Duration: 0.36mins

Typist comments regarding dictation: Mostly clear

VOICE FILE NAME: Meeting with CC03 (29 June, 2015)

Key:

I = Interviewer Woman

R = Respondent

aah = sounds like

I Good morning Mr. CC03 as we communicate via an e-mail. I'm doing a research about migrating healthcare services to cloud computing. Can you please introduce yourself and your role in the organisation?

R Well. My name is CC03. Senior solution architect. I'm also the government cloud manager in government cloud we actually more focusing in the basic infrastructure and building basic blocks of the cloud in IaaS, PaaS and SaaS. We might extended to Business PaaS.

I can you please clarify G-Cloud in more details?

R G-Cloud is a platform based on open source technologies that enables the Omani Government and other state authorities to locate their information systems to a central state-managed private cloud and to refrain from maintaining their own IT-infrastructures. The objective for implementing G-Cloud is to improve ministries' business outcomes by consolidating their IT infrastructure, reducing the IT budget and increasing their agility as well as to provide government ICT services at lower costs.

I Great, my research is basically about migrating healthcare services to cloud so that the patient will have his/her medical record available online with all medical history. Where is ministry of health standing from here. I heard they are deploying partly cloud in some of its services.

R aah .. not sure exactly what ministry of health is doing. But I do agree about that this will be defiantly a big jump in terms of quality in healthcare in Oman. aah another thing from what you've just said I have seen you have stepped one step ahead then what's cloud can offer. When we talk about cloud. cloud can be two things. From consumer point of view or citizens or residents point of view. It can be I'm user setting at home getting my information from the internet my status my information list. This is not just cloud player

over here. This is a complete integrated solution and application that can bring you the information. Which at this point can come from ministry of health. For example or maybe any private healthcare Bader Alsama or Star care whatever we have in the country. The cloud concept normally would help the organisation to speed up the process that means they can acquire infrastructure as a service (IaaS). They can provision platform as a service (PaaS) and go for software as a service (SaaS). Now how do they play and what kind of application they really want to put on it depends on their organisation strategy. What's ministry of health strategy. One of the application I can see which could have big potentials is the healthcare. You know unifying kind of information of course, security is important at this range but definitely, it will make simple to do it. But not sure if ministry of health publish anything that way in cloud yet. But I heard that they are working in such project that citizen and resident can now book their appointment for special hospitals and public hospitals in Oman. Please check with ministry of health, as I am not their representative so this question is directly for them.

I Of course I will double check from ministry of health in all cases I'm planning to see staff who work in IT department in ministry of health. So if we would like to talk about the security of the information as far as you are concern. Will the data or information in the cloud be encrypted (coded)

R Yeah definitely there are many ways of securing your information. Security itself is a huge chapter when of them starts from Infrastructure level where you need to secure your physical location where you put your VMs and hardware and data centers itself. And that's completely different method of doing it. Then you have the middleware where you need to check about VMs and some sort of application security related. Then you have the application layer where you have data transformation, data transactions happens between place A to place B and that's different way of securing. Now in cloud we actually following security standard like **NIST** security standard. Also we have government security standard, which is held by the one the division in ITA ensuring producing the national related security standard for Oman. hum.. This is also part of our main security divisions, which called, is the ISD. They actually responsible ensuring to security all of the data information that can come. There is a huge exercise to secure any information. Now going back to your project. Your project mainly comes to medical report and medical information. From my point of view as an ITA representative aah the information that we can secure is the information that related to entity that's very true. But the entity also need to come with their own security to consulate. Coz when we talk about information of X person in Oman who has so and so secret no one should know. Security comes true an application layer where the vender or implementer must have really taken a place and also it has to come to the middle wear and infrastructure layer. Now for us if they become part of the government cloud we secure all layer depending on what package they took . Let say if they took infrastructure as package we will be secure their infrastructure as well along with secure the rest but not as much when they took software as service when we provide the service the software then they just use it.

I okay so what you are saying you have different packages?

R Yes

I ok.. now the customer has the right to choose which package to use. Right. As far as I know ITA provide cloud service to various ministries free of charge?

R aah that statement not completely right. We provide cloud-computing services at this point to selective customers. When I say selective that means customers that fall under criteria and prerequisites. One of the main prerequisites they must have some sort of service

that service citizens and residents and integrated services with other ministries. to speed up the electronic Oman (eOman). That kind of project we currently looking for we do not have a target at this point for hosting a website. at this point is not our main focal. Maybe sometime in future but not now. That's why I said that statement is not completely true. When you said free I'm not sure also its free. Because there will some sort of cost. Because these infrastructure we are providing doesn't come free but we are not profitable organisation so we probably be much more cheaper than the rest. And from security point of view when they come to the cloud we are responsible to secure them. So also this another goal added and point to the project.

I So let assume that ITA provide cloud service to A ministry, they will be concern about their backup data, is monitored by ITA, will they have like incident report if anything goes wrong. Will it be listed in their agreement?

R Yes we have a SLA that we will signed with any customer who become part of our cloud customer and we will provide them definitely a complete monitoring systems. When we say monitoring system along with the operation we say they can raise a ticket any time they wants. They have the ability to see how they performing. What exactly went wrong in any certain time period. Coz we have back team in ITA responsible to see if anything goes wrong with their application so yeah that insurance we defiantly provide with SLA as well. So there will be customer agreement signed off and SLA agreed between us and there will be OLA as well (Operational Level Agreement).

I let say the customer is not comfortable about the service will it be available all the time let say network breaks during any natural disaster happen will they be able to access the service at that time.

R See if they took a package with DR as a services coz we have this service then DR will defiantly suits that kind of requirement. Which they can switch at any time to DR sites and the primary sites maintained.

I So what you are saying they can switch from one package to another one easily?

R They have to come with the first request what they want. If you are ministry X then you would know you need a backup. You would know any cluster environment. And you probably looking for DR service. So you put that as requirement *as it does not come as default* so you've got them all. Because when you start either migrating your application to the cloud or installing fresh insulation to the cloud. You must have basic structure design. How things should move when things went wrong right. According to the plan we studied with you, we will give suggestion if we can. From there if you have disaster from human side somehow you can always switch if you have package of the DR. if you actually backup coz the backup will come according what kind of backup you would like to have then that backup definitely be stored with us.

I Well I have two points to clarify. Will the data itself be coded when it stored in the cloud or according to the customer request.

R No it will not be encoded. Actually we have a department for coding and encoding. But now the encoding and decoding also depends on what the package you have. With infrastructure as a service we can't do much coz we are providing with the infrastructure. When we go to Software as service yes we encode and decode. When you go as platform as service we do encode and decode. But for security also reason if you are asking how secure is this we are running private cloud in ITA which means we have separate network. It is not public network like Amazon its not. It is separate network, which is secure by devices.

These devices one responsibility encoding and decoding data transformation defiantly that will be the case. And also from implementer point of view they normally make sure that the data is encoded and decoded as well.

I Ok let say the customer would request to delete his/her data in the cloud will it actually be erased?

R Yes. see about the delete and removed it depends exactly on what they are look if they wanna delete this question deal with how security is this right? .. I think if you have delete your VMs or your application and probably its at development stage right. you delete an application. And you haven't make a backup for this . then that defiantly it will be deleted. Let say If you go to production and say I want to delete a VM. Then deleting this is not that easy because you need to come up with approval to delete a production of data. The scenario here can go wide depending on what application you do. If you are talking about medical record data then defiantly for ITA we do not own it. Let say ministry of health host their applications or medical report within the GCloud then yes. Within GCloud they are as tenant but still not owning the data. For me setting in the operation room I cannot see what's in. I do not have the right to see what's in but you as ministry of health representative you can. So you can anything with your data as long as it's your business. And if you feel you want to correct data then still it's your business. I cannot come and say no you are not allowed. For me I provide you a service to facilitate you but not responsible on changing anything in your data.

I Alright.. let's assume that health ministry request the service and they have it. Regarding the access to the data. Will the patient has an access to his data in the cloud. Or it will be for hospital only.

R It depends on the design of the application of ministry of health. If they designed in a way the patient can access from the internet. Then yes, they will. But if they just come up with an application that can be designed internally with some sort of Ministry of Health centers then that's the way you can approach it. Each and every design for us we accept both. Now this is the thing the cloud I think the only confusion between your questions is the cloud and actually the accessibility of data. These two different things. The cloud is actually simplify for me as a ministry or government cloud to get infrastructure as service and it simplify to get platform as service. It simplify my life if I want to go for software as a service. Now it depends what kind of software let say you ministry of health and you took Infrastructure as service as a package where I install and I bring my application. That application probably with citizens and residents through internet to check their report. Then cloud will defiantly help it because they provide a system that capable to provide that service to resident and citizens. The cloud itself is there you can use it and do anything with it. I'm not sure if I did help you with my answer but I'm trying to tell you that actually your question has two different path. One path is application related question where I think an application architect within ministry of health should tell you what's going on right now about their projects that services citizens and residents. Another question I'm answering here is what cloud would help this application in order to make this story true and invisible for citizen and residents.

I Well I'm trying to get some people from ministry of health in order to question where are the standing from migration healthcare services to cloud computing will they be interested or not. Lets go back to security if there is an incident report.. will you notify the customers that so and so had happen in such date ? and those reaction where taken and dealt with?

R Yeah ..notification again task number one you are asking for is notification in the application it should be yes happening but that related to the ministry from our point of view will notify them according to what package they have. Let say they have a problem with their VMs we tell them. But if there is an application the one they design has stuck or loop within the application that we cannot tell. But we can tell them if they have performance problem. Application related its not owned by us its not we are not providing then it will be ministry of health especially when it go to medical related application then they take a complete security aspect for it. But from government cloud point of view we do give them a complete notification that related to their package.

I In terms of your services that you are providing to the ministries. Is there like audit and run by who.

R Yes, we are running an internal audit within ITA and as you can cloud itself. It is very flexible in terms of demand. If you ask one VM server, you can get it within 5 minutes. Sometimes you have projects that run seasonally for example Majles Alshura someone wanna just see a vote of something in probably one month. So they are asking for so and so service. That only required for one month. The flexibility of the cloud you can get all of these VMs at once. And when the job is done you can say close I do not need them anymore maybe next year again. So you get the flexibility of resources. That will defiantly will help to provide ministries their own demands .we call it on-demand-services. About the audit actually we do have an audit about how many customers do we have and also about our infrastructure we are running internally. So yes we defiantly do. How we run it you mean? Actually there are many many ways.

I Ok great .. I wonder if you do outsourcing for some the services in cloud as you said you are capable provide different packages according to the customer need.

R I would say we will be able to run PaaS at this point we are providing infrastructure as a service (IaaS) in a month and half time we would be probably running PaaS and early next year we will provide SaaS.

I Excellent .. aah we talked about technical issues whether isolation failure might occur

R Yes the isolation failure depends exactly on what categorise but defiantly we are taking care of all the operations requirement. When we talk about operation requirement we can sum it from infrastructure point of view operation monitoring and also support.

I What about the legal agreement who provide SLA ?

R We are provide SLAs. And agreement must be signed by the tenant or ministries.

I Are you expecting any kind or risks not precisely related to the cloud? Aah as we said natural disasters attacks.

R Yeah defiantly I mean that was why we are putting DR service in different locations in case this cloud has problem then the other cloud will run straight away.

I aah .. thank you so much ..

R You wanna ask about outsourcing something

I Oh yeah thanks .. I meant for outsourcing some of the cloud services do you rely on other providers to do the service?

R No strategically this point as government we really want to run the service for the tenant in secure environment we are not outsourcing any other cloud from different vendors like amazon .we build the cloud within our data centre. But in future if we found some sort of venders that could bring potential and secured. Yes we are also ready because we have cloud connector that can connect to any other cloud later .

I So what you said regarding the location not necessary to be here in Oman?

R No at this point we do not have outside all in Oman because of security promising it should be in Oman. as I said at the beginning we have to follow the government security rule that information security rules released in 2013. But it been released by our security advisor division in ITA. And we follow that.

I Is there any documentation or statistics who used the cloud service from ITA so far.

R Well to be honest we just started with three customers yet. So the statistics not clear yet even for us. We are trying to get complete statistics. But I think at the end of this year we will be able to announce a complete statistics and how we are performing and defiantly it will be publicly shared.

I So at the end of year I will contact you again to it that statistics hopefully.

R Alright..at this time we have two major projects one of them is eOman itself in cloud and the other one is ministry of health and there is few 8 to 12 ministries potentially coming as well to cloud in various packages.

I aah .. whom do you recommend to meet next regarding the same area.

R I think most of your questions will defiantly be answered by ministry of health because your project is about providing a shred service for resident and citizens in Oman that they can access their medical report. Now this medical report can set on the cloud or in their premises it does not matter. Because your goal is how to make those recorders available to public which is fall into shared services area. Aaah defiantly ministry of health can give you where they are and maybe they can tell you if they have sort of challenges at this moment. I'm not aware about it. Aah but I know they would answer most of the questions. Because most of my answers how we can help X ministries to give what you are asking for. But now even with the cloud if X ministries or entities are not ready to accommodate those services to citizens and residents. You are citizen wont feel the reason behind why we are doing a cloud.

I Well to convince a manager or undersecretary about the facilities within the cloud obviously we need to clarify the cost of it. Do you have an idea how much each package cost? How cloud can save a lot of expenses to them .

R The pricing not yet released as I said we are not profitable organisation. The only reason we are running the cloud to speed up the shared services in Oman. Whoever tenant come in us is basically to speed up the process of giving those services to citizen and residents. We are not profitable so our price will be the lowest among others. The numbers I do not have them yet no one has them yet. As you we just started we've gone life two months back. We have two customers so far

I May I know who those customers are ?

R Yeah eOman project and Ministry of Health.

I Whom shall I contact in Ministry of Health

R aaah .. not about the same project .. its different than what you are asking for it called “Shefa Project”. I probably I can share the contact person but I need to ask first.

I Yes please do. I can leave you with my number and e-mail.

R What I think you should do is go to Ministry of health to IT department and ask about shared services to citizens and residents and where we are at this point. They will tell you probably what they have. You will be surprized of what we have but no one is using it.

I no one is using it !!

R Yeah there are two thing; we have but no one knows about it. And we have but it useless because no one can use it and we can not have because challenges. We defiantly see those when you set with them. So the point is not go to project related to us as much as IT central IT with ministry of health asking for that questions. Probably you will get better answers for your questions.

I I think they should market their service so the public will know about and go ahead and use it.

R Marking is actually one of the reason that the citizens and residents use the service. But it depends on what do they have and how much they can.. there are much complexity when it come to shared service. I think by the end of this research you will probably know most of them and you go and understand why it was not possible at so and so time and why it possible now. And you will see that challenges. Myself I do not even know how much do they achieve because we do not go in details in cloud. but I’m sure there is a division in ITA do have a good idea what they are doing. Like e-services team who have statistics because they are responsible on government services. They doing a survey about readiness. That report will come from e-services team. You might be able to see the e-health readiness if can ask for that report. Then they can tell where they are at this point because they run that exercises. It is a different division than government cloud.

I Most of the public when you ask them to use e-services they comment on the internet speed as not efficient to perform such tasks.

R Infrastructure speed can be also a bottleneck but it depends on what you want to share. Infrastructure might have ... not just in Oman anywhere in the world by the way because you would always want to improve the speed of the performance. But the architecture design that you can come up with can serve citizen and residence according to what do you have of the infrastructure limitation. Does not mean I have to wait 10 years or so until I see the infrastructure grow up to certain level then I can act. We started by iminium computers and we able to come up to where are right now. Technology moves along. The good architect, good design, good thought of what kind or services I can provide to publicly for citizens and residents leads to an answer but that’s again depends on what’s your objectives about the project.

I well so my next aim is to target people on shares services in ministry of health.

R Right .. or one of the team of e-health readiness. So first, you get one of them here then you see the people from health ministry.

I Thank you so much for your time. I really appreciate it.

R You welcome my pleasure to help.

A.6 Interview Transcript with CC04

Interview transcript no 4

Date: 20th Sep, 2015

Voice file name: Meeting with CC04, Director of eHealth in ministry of health in department of IT

Duration: 0.20 mins

Typist comments regarding dictation: Mostly clear

VOICE FILE NAME: Meeting with CC04 (16 August, 2015)

Key:

I = Interviewer Woman

R = Respondent

aah = sounds like

I Good morning my name is Aseela Al Harthi and I'm doing a research about migrating healthcare services to cloud computing. Can you please introduce yourself and your role in the organisation?

R Ok. My name is CC04 . Director of eHealth in Ministry of Health in Department of Information Technology. I'm responsible for eHealth portal.

I Did you really start migrating healthcare service to cloud or not yet?

R "We are not providing eHealth services in terms of health services. We are providing e-services in terms of just communicating what health establishment. to request an appointment or can cancel an appointment or reschedule an appointment. We do not store the medical records of a patient online. Doctor can view patient chart as long as the patient is under his care. In case you are admitted in the hospital and his away not in duty and he needs to be consulted for something then he can view it from outside.

I Can the patient view his/her chart outside Oman or only within Oman.

R He can view it outside Oman as long as he has internet connection and log in with his Id card.

I This Id card will it has patient medical history from various hospitals in Oman. as you know the patient database in Khaula Hospital is different than the one in Alsultani Hospital. So a patient will have a record in both hospitals.

R The Id card does not store the medical history. It is read from Archive of health information system through the portal. And it read chart by chart it doesn't read a combination of both records so far. Because still did not unified the patient record. We will be doing in stages later.

I So let say cloud service will be a solution to unified the patient records?

R Actually no we are not utilizing the cloud solution to unify the records. we are doing it in data base level.

I When you do it in database level moving to electronics records. will it minimize some of the departments role?

R Like what?

I Like some departments like patient registry or storage data.

R Still not clear sorry

I Ok let say patient A has a medical record in Khula Hospital and would like to take a second opinion from one of the private establishment (Bader Alsama) his electronic medical records or chart will it be viewable to the doctor?

R Right .. at this stage no we do not give access to the patient chart through the portal except for the patient or for the doctor who treat that patient in that hospital. So private establishment not included. But the patient himself can view the chart even from his mobile phone and then show it to the doctor but not on doctor PC.

I Do you think this system is secure?

R aah.. we have moved to GCloud as we are seeking more security. Because we do not have here the infrastructure and people to managed it. That's why we choose to use the GCloud for the portal I mean not for patient chart. Patient chart still client server. So it is locally in each hospital

I Let say there is an incident or security breach will you notify your patient that there is a breach in the system?

R aah ..i can not speak for that. If its for the portal then it will be handled as soon as possible.

I Alright .. what about the patient chart in the system if you request certain data to be deleted is actually removed or erased from the system.

R We do not store anything in the portal. We send web service request and get whatever data stored in it.

I I would like to know more how you will use GCloud in health portal

R Basically we are hosting the application or the system of eHealth portal in the cloud. We are utilizing their environment as the infrastructure already there. we are using the ITA government cloud to host the ministry portal (website)

I So you will use the cloud infrastructure to make eHealth portal accessible and useable.

R Yeah for hospital and administrative staff.

I Do you something called Alshefa project? What it is about?

R Alshefa is electronic health record. It is client server based. It is basically the patient chart. It covers everything from patient registration to examination, radiology, tests, x-rays. Each hospital has its own local database on site

I Great and those data will it be stored in Alshefa?

R The data will be stored locally in each hospital. It build in oracle system. So the portal is web service only it request for patient data only.

I What about the storage capacity? Will it have enough storage for each patient data?

R Do you mean Alshefa ? yeah I think they have enough. I can not speak for them as it is different department.

I Right .. how can I get more details about Alshefa project and eHealth portal?

R For al Alshefa you need to speak to different department called health applications but for eHealth I can provide you with the information. As for the eHealth portal basically it is our website but its been updated.

I Right .. I will add your name for eHealth portal.. I will need to know the main objective of it and at what stage you are in right now. I will give my contact details.

R Ok I can send all the details to you via an e-mail .

I Great .. thank you so much for your time .

A.7 Interview Transcript with CC05

Via e-mail

Category	Question list
Role in the organization	<p>1. What are the roles you play in the healthcare organization(s)? Give more details about each role. Dr. CC05, Assistant professor, Science College at Sultan Qaboos University</p>
Management perspective	<p>2.What do you think about migrating healthcare service to cloud?</p> <p>Migrating services to clouds becomes more and more attractive IT option to cut costs, support on-demand provisioning, diversify infrastructures, and obtain higher levels of flexibility and security</p> <p>3. Would system administrators be happy to give up some of their control over systems and rely on cloud service providers for the support of end users?</p> <p>It varies from one to one. Although I think migrating partially to Cloud computing will give them a chance to inspect the reality of what cloud can and can't do.</p> <p>4.How would departments react to the migration of applications and data to cloud service providers? Several concerns have held healthcare organizations back from moving ahead toward full-scale cloud migrations. Examples of such concerns are privacy and security.</p> <p>They might not have the same level of access to a cloud as they currently do to their internal systems, so how would they have to change their working practices? They still can manage the cloud.</p>
Security (Data storage, process and transfer)	<p>5.What do you think the role of security is/ should be in healthcare? The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures</p> <p>6.What is the backup plan for data stored in the cloud?</p> <p>7. Will the data be encrypted in the cloud? How will it processed or transferred?</p> <p>8.Will the data be isolated?</p> <p>9.Can the data be portable to different cloud provider? How long it will take to migrate to another cloud? Is there a special tool for exporting data?</p> <p>10.Does your cloud service provide data integrity and availability?</p>

	<p>11.How the original data be deleted? Is it actually erased when contract terminated.</p> <p>12. Is it monitored? From provider to ensure acceptable use and customer Can the data be Non-repudiation?</p> <p>From my side I think cloud provider should provide backup, encrypt data, make it portable and provide data integrity</p>
Security (Access control)	<p>13.Does your cloud provider provide management access control within healthcare? N/A</p> <p>14.does your cloud provider have “backdoor” for maintenance, support and services N/A</p> <p>User/patient access control in the healthcare</p>
Security (procedure)	<p>15.Does your cloud provider provide “Auditing” N/A</p> <p>Certification (customer to check is it relevant to their work or not) and does it follow Personal Identifiable Information(PII) ISO/IEC 27018:2014</p> <p>16.Countermeasures- how does your cloud provider react about security breach? N/A</p> <p>17.Testing (cloud provider what kind of security tests) N/A</p> <p>18.If there is breach of security will the provider provide a notification to customers or not? Detection Key management Security level</p>
Incident management	<p>18.How security incident are dealt with? Does cloud provider provide: Response? Logging? Reporting? Forensics?</p> <p>19.Is there a certain mechanism to notify customers about data breaches or information security incident?</p>
Privacy	<p>20.Non-disclosure? Can provider use or access the data? N/A</p> <p>Data minimization</p>
Hybird clouds	<p>21. Does your cloud provide rely on outsourcing some of the services? (may rely on the services from multiple provider) N/A</p>

Technical	<p>22. Does your cloud provider face or likely to some of the following technical issues? if yes, how it deals with? Resource exhaustion (under or over provisioning) Isolation failure Cloud provider malicious insider- abuse of high privilege roles Management interface compromise (manipulation, availability of infrastructure) Intercepting data in transit Insecure or ineffective deletion of data Distributed denial of service (DDoS) Economic denial of service (EDOS) Loss of Cryptographic Keys Compromise service engine Conflicts between customer hardening procedures and cloud environment N/A</p>
Legal	<p>23. Does your cloud provider clarify the status of the legal issues for instance: Risk from changes of jurisdiction Data protection risks Licensing risks N/A</p> <p>24. Does your cloud provider follow Health Insurance Portability and Accountability Act (HIPAA)? N/A</p> <p>25. Does your cloud provider follow Personal Information Protection and Electronic Documents Act (PIPEDA)?</p>
Risks not specific to the cloud	<p>26. Does your cloud provider face or likely to some of the following issues? Network breaks Network management (network congestion/mis-connection/non-optimal use) Modifying network traffic Privilege escalation Social engineering attacks (impersonation) Loss or compromise of operational logs Loss or compromise of security logs (manipulation of forensic investigation) Backups lost, stolen Non Cloud-Specific Network-Related Technical Failures or Attacks Natural disasters N/A</p>
Further recommendation	<p>27. Do you recommend anyone who we can speak to about the areas we mentioned above? (For example, those dealing with Information Governance, Health Information systems, or cloud provider) ITA g-cloud team</p>

A.8 Interview Transcript with CC06

Via e-mail

Category	Question list
Role in the organization	<p>1. What are the roles you play in the healthcare organization(s)? Give more details about each role.</p> <p>Dr. CC06, Assistant Professor and healthcare consultant and manager. As a health care manager I command the operation of different types of medical facilities. They typically work closely with medical staff as well as industry suppliers and others involved in the delivery of health care. Some important roles are;</p> <p><u>Strategic Planning</u>: The manager is in charge of making business decisions and leading strategic planning to create a vision and direction for the practice or facility going forward. He normally works with medical boards and the medical staff to make sure the clinic's goals align with that of the budget, community needs and practitioner goals.</p> <p><u>Spokesperson</u> : When media seeks information from a medical facility, the manager normally serves as the organization's spokesperson. Some large hospitals have full-time spokespeople or public relations representatives, though. In this capacity, the manager holds press conferences or delegates delivery of press releases to announce important news or events.</p> <p><u>Collaboration</u> :The health care manager typically collaborates with medical staff leaders to coordinate ongoing and daily responsibilities. He coordinates departmental budgets with each department head, discusses medical equipment and supply needs with physicians, and delegates and follows up on any tasks related to the overall operation of the practice. Maintaining good rapport with physicians and nurses is a key duty of health care managers to keep morale high.</p> <p><u>Staff Management</u> :The health care manager also has oversight over staff and helps run daily operations of the facility. This includes office staff, billing departments, doctors and nurses and custodial staff. This is one of the more challenging roles of the manager, as he must make critical decisions on what the facility's budget allows for help, what standards are in play for performance, and how to evaluate the performance of each type of worker.</p>
Management perspective	<p>2. What do you think about migrating healthcare service to cloud?</p>

Answer: The rate of adoption of cloud computing technologies is rising rapidly and there doesn't seem to be any signs of it slowing down. Cloud Computing quickly brings in natural economies of scale with most cloud services provider charging on a pay as you go basis thereby eliminating wastage on unused resources. Many healthcare organizations embark on cloud migrations to achieve scalability, cost-efficiency and higher application performance healthcare services. But migrating apps to the cloud is a complex process that requires careful planning and deliberation. It's essential that healthcare organizations consider all possibilities -- both good and bad. Cloud migration issues, such as unexpected costs, interoperability, security gaps and unanticipated application rework, can create significant obstacles. To help smooth a frequently bumpy path, healthcare organizations need to craft a well-thought-out migration strategy.

Whether your organization is migrating to the cloud from an in-house environment, it's important to understand the process and temper any exorbitant expectations. And, since not every application will benefit from the cloud, make sure a migration is right for your organization before diving in.

3. Would system administrators be happy to give up some of their control over systems and rely on cloud service providers for the support of end users?

Answer: The systems administrator role is perhaps one of the earliest in technology, at least as far as the implementation of a system goes. In the earliest days of computing, electronic technical professionals built prototype computers, and newly minted "programmers" wrote logical instructions for these systems. In time, the systems administration role owned the installation, configuration, operation and tuning of these systems once they went into production and use on a larger scale.

The systems administrator has the same concerns and impacts of "the cloud" as the DBA and the Systems Architect. They need to educate themselves on the options within this new option (Knowledge), try a few test solutions out (Experience) and of course work with others on various parts of the implementation (Coordination).

4. How would departments react to the migration of applications and data to cloud service providers? They might not have the same level of access to a cloud as they currently do to their internal systems, so how would they have to change their working practices?

Answer: When departments are migrating towards cloud service they usually face many challenges which are; incompatibility issues, security and privacy issues, reliability issues, availability issues and network connectivity issues etc. So, by underlining these issue it seems difficult to migrate from internal systems to cloud but once the department staff is trained then they will understand the full value of cloud system. For the purpose of staff training department

	<p>must offer them different certifications, workshop and educate them to understand work flow of cloud system. Once the staff is become, user friendly with cloud system working practices then they might be on the level to take benefits of cloud facilities.</p>
<p>Security (Data storage, process and transfer)</p>	<p>5. What do you think the role of security is/ should be in healthcare?</p> <p>Answer: Role of <u>security</u> is important to protect patient privacy, comply with health care laws, and ensure that only authorized health care professionals access the correct data. Some health organizations are hesitant to adopt cloud computing because of the complexity of structuring cloud computing to comply with the Health Insurance Portability and Accountability Act (HIPAA), which regulates how health organizations protect private healthcare information. Others are resistant to adopting cloud computing due to concerns over unauthorized access to data. Patients are not always viewing their medical records online due to <u>network security concerns</u>.</p> <p>A successful cloud healthcare network must use data security measures that comply with HIPAA, prevent unauthorized access, and protect authentic patient data. There must be no doubt of the authenticity of patient data, which can make the difference in effective medical treatment. Both healthcare professionals and patients must trust the cloud network security to protect personal data for it to work. Effective cloud security will gain this vital trust.</p> <p>Challenges of Cloud Security: Effective cloud security must address key challenges in the following areas:</p> <p>Preventing unauthorized access: It is critical that only authorized users' access data in a healthcare setup. This can be tricky in a virtual environment with so many remote users and multiple Wi-Fi devices.</p> <p>Accessing data safely from mobile devices: Health professionals and patients should be able to access data securely from mobile devices like cell phones, tablets, or laptops. If network security isn't optimal, vulnerable data could be lost or stolen when accessed through an unsecured mobile device.</p> <p>Protecting databases from malware and attacks: A cloud must have a secure database that effectively protects against cyber attacks and malware. Some popular security components like open-source software, which played a role in the Heart bleed bug breach at Community Health Systems, are not the safest options. It is also important to have an incident repair and response system in place to respond quickly to block any attacks or breaches.</p> <p>Preventing data loss: A cloud has to have a good system to prevent data loss and a way to retrieve lost data when possible. A cyber-attack, an encryption error, or a natural disaster are some of the ways data could be lost.</p> <p>6. What is the backup plan for data stored in the cloud?</p> <p>Answer: Cloud backup, also known as online <u>backup</u>, is a strategy for backing up data that involves sending a copy of the data over a proprietary or public network to an off-site server. <u>The server is usually hosted by a third-party service provider, who charges the</u></p>

backup customer a fee based on capacity, bandwidth or number of users.

Online backup systems are typically built around a client software application that runs on a schedule determined by the level of service the customer has purchased. If the customer has contracted for daily backups, for instance, then the application collects, compresses, encrypts and transfers data to the service provider's servers every 24 hours. To reduce the amount of bandwidth consumed and the time it takes to transfer files, the service provider might only provide incremental backups after the initial full backup.

Third-party cloud backup has gained popularity with small offices and home users because of its convenience. Capital expenditures for additional hardware are not required and backups can be run dark, which means they can be run automatically without manual intervention.

7. Will the data be encrypted in the cloud? How will it processed or transferred?

Answer: Yes data will be encrypted in cloud because encryption changes data into a secure format that only an authorized user with the correct encryption key can access. Data should be encrypted when it is in use, in transit, and at rest to make sure that the data is unreadable if it is lost or stolen. Split-key encryption provides even greater network security because it is protected by two encryption keys, which are held by the healthcare organization and the cloud service provider. Both keys must be used in order to access data.

8. Will the data be isolated?

Answer: Yes, data Isolation can be seen as a special sort of privacy, where the a service should not get in contact with other services, and the provider of the Cloud should not know what data are used in the service and for what purpose the service is used by the customer.

9. Can the data be portable to different cloud provider?

How long it will take to migrate to another cloud?

Is there a special tool for exporting data?

Answer: Yes, Data can be portable or migrate to different cloud provider, Moreover the migrating time depend the size of the data, hardware capacity and network bandwidth. There are also some special tools for exporting data from cloud to cloud one of these tool is Nava Certus 1.4 (<http://www.linkgard.com/blog/cloud-storage-migration-is-becoming-a-serious-business.html>). Some of cloud to cloud migration tactics are listed below;

1. Direct cloud-to-cloud migration: Some providers have direct, high-speed connections to other providers. For example, Google and TwinStrata have worked together to develop a way to migrate data from one cloud to the next using Google's own high-speed

connections, and without any impact on the customer's network. Once the data is moved, it's a fairly simple exercise to maintain access to the data using TwinStrata Cloud Array - without having to modify any of your application settings. And in fact, that's exactly what we did for customers such as IAC in the last few weeks.

2. Cloud compute migration: One of the fundamental advantages of using cloud-integrated storage is the ability to spin up the software in the cloud. By spinning up your cloud gateway in a cloud compute environment, you can do the migration from one cloud to the other using without taxing your own network.

3. Re-point the cache: For some organizations, an on-premise transfer is unnecessary. Some of our customers (particularly those using cloud for backup or application data) keep a full copy of everything they have in the cloud in their local cache. If you're accessing the cloud through a cloud gateway, you should be able to just re-point the cache to the new provider, thereby limiting the impact on your network to just outgoing traffic.

4. On-premise transfer: If the amount of data you have in the cloud is small, and your corporate network is large, you can bring the data back on premise and then send it to the new cloud of your choice. If you're using a cloud enabler such as TwinStrata's cloud-integrated storage software CloudArray, this exercise becomes significantly simpler because you can simply migrate the volume to another provider, but it can take a toll on your network.

5. Start fresh: The final option is limited to those customers who use cloud storage to back up their on-premise data. A small number of organizations with which we've worked have elected to start fresh with a new cloud provider by copying their on-premise backups to the new cloud, Once it is safely migrated, they can then delete the data from their existing cloud (or in the case of Nirvanix, just throw away the encryption keys so it can't be accessed). This option is viable only if you're using the cloud for backups and have enough onsite copies of your backup to meet your retention policy.

10. Does your cloud service provide data integrity and availability?

Answer:

Cloud Service Data Integrity: Yes, cloud service data Integrity should be computed for every document and kept in the database. The encryption mechanism used to ensure confidentiality during the TCP/IP transmission includes an integrity check that prevents the risk of data corruption. A typical integrity check is the use of hashes. Hashes can be included in a signature to ensure authenticity. In such a case, the signature contains the document hash encrypted with the sender private key and the public key to allow decryption. It also points to the certification authority. The key used to encrypt the data should be stored (encrypted) with the data itself. If data has been modified intentionally, or accidentally, data decryption would then fail. This protection also prevents the sending of corrupted data to clinicians and other users.

Cloud Service Availability: In cloud service availability any service or application should start with a secure and reliable storage mechanism:

- The cloud service provider should maintain at least two copies of ingested data, thus reducing the risk of data loss. One of the two copies is made on removable media so it can be stored at another location—in case a disaster impacts the data center. The system should ensure that the two copies are permanently synchronized.
- Database is stored on RAID-10 (1+0) disk system. RAID-10 provides high availability and performance when there is a need to reconstruct data in the case of disk failure.
- Data is stored on RAID-6. While this type of RAID is slower to reconstruct in case of disk failure, it offers excellent reliability with a higher ratio of usable storage/physical storage.

One of the often overlooked areas of data security is authentication procedures. It is not enough to maintain two copies of patient data—the cloud service provider must also have a validation process that ensures that each copy of the data maintains its integrity. Damaged files must be able to be detected and reconstructed. Responsibility for maintaining data integrity should be clearly defined as part of any contract with a service provider.

11. How the original data be deleted? Is it actually erased when contract terminated.

Answer: Data deletion is also of prime importance when terminating the contract with the provider. An essential point is that data that has to be deleted by the user because he or she no longer needs it or may no longer process it for another reason is also deleted by the provider and no more copies of data are available. This can lead to problems, in particular in connection with backups that are created by the provider if these contain data belonging to a number of his customers and targeted deletion of individual data items proves financially unreasonable or technically inappropriate in terms of feasibility.

As far as the Data Retention policy of the cloud service provider is concerned, the law against which the state's jurisdiction falls into is also of prime importance. For example, The Health Insurance Portability and Accountability Act of 1996 mandates the retention of data for 6 year. Once, the data exceeds the specified period of retention, it's critical to ensure its safe disposal. The Federal Trade Commission's FACTA Disposal Rule mandates that the data be cleaned up should it be deemed of no use. Another example would be The General Data Protection Regulation proposed by the European Commission which provisions for a "Right to Erasure".

	<p>12. Is it monitored? From provider to ensure acceptable use and customer Can the data be Non-repudiation?</p> <p>Answer: Non repudiation of data over the cloud can be ensured in several ways. The easiest of which would be to determine the proof of data integrity. This may be accomplished via the checking of data hash. Alternatively, the method of using Digital Certificates may also be used to ensure the origin of a particular data stream and its authenticity.</p>
Security (Access control)	<p>13. Does your cloud provider provide management access control within healthcare?</p> <p>14. does your cloud provider have “backdoor” for maintenance, support and services</p> <p>User/patient access control in the healthcare</p>
Security (procedure)	<p>15. Does your cloud provider provide “Auditing”</p> <p>Answer: Yes, because by agreeing on information and audit rights, the user establishes the opportunity to verify that the obligations entered into by the provider are being fulfilled. Depending on the sector to which the user belongs, such rights also have to be provided for auditing companies and regulatory authorities to whose control the user is subject.</p> <p>Certification (customer to check is it relevant to their work or not) and does it follow Personal Identifiable Information(PII) ISO/IEC 27018:2014</p> <p>16. Countermeasures- how does your cloud provider react about security breach?</p> <p>Answer: In general, they follow these steps to reduce the risk of suffering security breaches:</p> <ol style="list-style-type: none"> 1. Authenticate all people accessing the cloud. 2. Frame all access permissions so users have access only to the applications and data that they’ve been granted specific permission to access. 3. Authenticate all software running on any computer — and all changes to such software. 4. Formalize the process of requesting permission to access data or applications. 5. Monitor all network activity and log all unusual activity. 6. Log all user activity and program activity and analyze it for unexpected behavior. 7. Encrypt, up to the point of use, all valuable data that needs extra protection.

8. Regularly check the network for vulnerabilities in all software exposed to the Internet or any external users.

17. Testing (cloud provider what kind of security tests)?

Answer: Cloud Testing uses cloud infrastructure for software testing. Organizations pursuing testing in general and load, performance testing and production service monitoring in particular are challenged by several problems like limited test budget, meeting deadlines, high costs per test, large number of test cases, and little or no reuse of tests and geographical distribution of users add to the challenges. Moreover ensuring high quality service delivery and avoiding outages requires testing in one's [datacenter](#), outside the data-center, or both. Cloud Testing is the solution to all these problems. Effective unlimited storage, quick availability of the infrastructure with scalability, flexibility and availability of distributed testing environment reduce the execution time of testing of large applications and lead to cost-effective solutions.

Types of Cloud Testing

Stress

Stress Test is used to determine ability of application to maintain a certain level of effectiveness beyond breaking point. It is essential for any application to work even under excessive stress and maintain stability. [Stress testing](#) assures this by creating peak loads using simulators. But the cost of creating such scenarios is enormous. Instead of investing capital in building on-premise testing environments, cloud testing offers an affordable and scalable alternative.

Load

[Load testing](#) of an application involves creation of heavy user traffic, and measuring its response. There is also a need to tune the performance of any application to meet certain standards. However a number of tools are available for that purpose.

Performance

Finding out thresholds, bottlenecks & limitations is a part of [performance testing](#). For this, testing performance under a particular workload is necessary. By using cloud testing, it is easy to create such environment and vary the nature of traffic on-demand. This effectively reduces cost and time by simulating thousands of geographically targeted users.

Functional

[Functional testing](#) of both internet and non-internet applications can be performed using cloud testing. The process of verification against specifications or system requirements is carried out in the cloud instead of on-site software testing.

Compatibility

Using cloud environment, instances of different Operating Systems can be created on demand, making compatibility testing effortless.

Browser performance

To verify application's support for various browser types and performance in each type can be accomplished with ease. Various tools enable automated website testing from the cloud.

Latency

	<p>Cloud testing is utilized to measure the latency between the action and the corresponding response for any application after deploying it on cloud.</p> <p>18.If there is breach of security will the provider provide a notification to customers or not? Detection Key management Security level</p>
Incident management	<p>18.How security incident are dealt with? Does cloud provider provide: Response? Logging? Reporting? Forensics?</p> <p>19.Is there a certain mechanism to notify customers about data breaches or information security incident?</p>
Privacy	<p>20.Non-disclosure? Can provider use or access the data?</p> <p>Answer: A non-disclosure agreement (NDA) is a signed formal agreement in which one party agrees to give a second party confidential information about its business or products and the second party agrees not to share this information with anyone else for a specified period of time. Non-disclosure agreements are common in technology companies where products are sometimes jointly developed. (In this case, the non-disclosure agreement is often mutual or two-way.) An NDA is also sometimes used when a company seeks venture capital from potential financial backers as a way to make sure that proprietary secrets or ideas are not stolen or leaked to someone else by the prospective investors.</p>
Hybird clouds	<p>21.Does your cloud provider rely on outsourcing some of the services? (may rely on the services from multiple provider)</p>
Technical	<p>22. Does your cloud provider face or likely to some of the following technical issues?if yes, how it deals with? Resource exhaustion (under or over provisioning) Isolation failure Cloud provider malicious insider- abuse of high privilege roles Management interface compromise (manipulation, availability of infrastructure) Intercepting data in transit Insecure or ineffective deletion of data Distributed denial of service (DDoS) Economic denial of service (EDOS) Loss of Cryptographic Keys Compromise service engine Conflicts between customer hardening procedures and cloud environment</p>

Legal	<p>23. Does your cloud provider clarify the status of the legal issues for instance: Risk from changes of jurisdiction Data protection risks Licensing risks</p> <p>24. Does your cloud provider follow Health Insurance Portability and Accountability Act(HIPAA)?</p> <p>Answer: Yes, because HIPAA is a U.S. Federal law that was designed to protect patient privacy, and does so by mandating and enforcing strict privacy and security rules over how medical information is collected, handled, used, disclosed and protected. While the HIPAA Privacy rule pertains to patients’ privacy and rights for their personal health information, the HIPAA Security rule, focuses on assuring the availability, confidentiality, and integrity, of electronic protected health information through a series of administrative, physical and technical safeguards.</p> <p>25. Does your cloud provider follow Personal Information Protection and Electronic Documents Act (PIPEDA)?</p>
Risks not specific to the cloud	<p>26. Does your cloud provider face or likely to some of the following issues? Network breaks Network management (network congestion/mis-connection/non-optimal use) Modifying network traffic Privilege escalation Social engineering attacks (impersonation) Loss or compromise of operational logs Loss or compromise of security logs (manipulation of forensic investigation) Backups lost, stolen Non Cloud-Specific Network-Related Technical Failures or Attacks Natural disasters</p>
Further recommendation	<p>27. Do you recommend anyone who we can speak to about the areas we mentioned above? (For example, those dealing with Information Governance, Health Information systems, or cloud provider)</p>

A.9 Interview Transcript with CC07

Feedback from Gartner representative via e-mail

The short answer to many of these questions is that if it is a private internal cloud you will have control over policies, procedures and design, thus it would be the design decisions as to whether or not you chose to create and store audit logs, what to do in the event of a security incident, an attack or a breach will necessarily have different responses.

If using public cloud then you are more restricted to what the provider either offers or is willing to negotiate on. For example some will allow government officials to inspect and audit the data centre, some will not.

Specific answers below in **Red**.

Category	Question list
Management perspective	<p>1. What do you think about migrating some services to cloud? (for example ROP or healthcare services)</p> <p>This is becoming the defacto operating model across many parts of the world. Many governments are now enacting “cloud first” policies, that is to say that government agencies are expected to use cloud computing in the first instance, and only not use it if there is a strong business case against. Simply saying security issues exist is no longer sufficient, as many would argue that public cloud from the big providers is MORE secure than many government agency data centers.</p> <p>2. Would system administrators be happy to give up some of their control over systems and rely on cloud service providers for the support of end users?</p> <p>Asking someone to give up part of their job is always difficult and human nature shows that a defensive position is often taken as people do not like change. That said many System Administrators are finding their roles developing, as they become cloud brokers. Responsible for sourcing and integrating the different cloud solutions being used.</p> <p>3. How would departments react to the migration of applications and data to cloud service providers? They might not have the same level of access to a cloud as they currently do to their internal systems, so how would they have to change their working practices?</p> <p>They do have the same level of access to systems and data to USE the application. Many departments welcome use of cloud based applications as they frequently offer more modern capabilities, frequent upgrades keeping the functionality current and they are not waiting on IT to deliver this. You need to be careful that these upgrades come at a pace that the organization can cope with in terms of training staff in the new functionality.</p>
Security	4. What do you think the role of security is/ should be in ROP?

<p>(Data storage, process and transfer)</p>	<p>I can't answer what it is, I am not familiar, but what it should be I could suggest the following.</p> <ul style="list-style-type: none"> • Setting policies and standards • Evaluating solutions and vendors • Auditing security and investigating data breaches and attacks if warranted. • Contributing to the classification of data and ensuring APPROPRIATE safeguards are in place for each level. This does not mean treat all data at the highest level which is what tends to happen as people seek to protect themselves from blame. • Openly discuss risk management NOT risk elimination. <p>5. What is the backup plan for data stored in the cloud? If it is your cloud it depends on what you decide, if it is in the public cloud it depends on the vendor's policy and what you are willing to pay/negotiate for. Do not assume because it is in the cloud it offers DR capabilities, but many do use the cloud for exactly this purpose.</p> <p>6. Will the data be encrypted in the cloud? How will it processed or transferred? If it is a private cloud it is your choice. If a public cloud that depends on the vendor and what service you are buying.</p> <p>7. Will the data be isolated? Your cloud your choice as to the degree of separation. The public cloud offers choices, multi-tenant where the separation is carried out at the software level and bars one user from seeing anothers. You can have single tenant where the hardware is dedicated to one organization offering physical separation. Finally you may choose to use a community of government cloud type model where different agencies or departments many share the same infrastructure and share data more easily but still in line with access rights, privileges'and agreements.</p> <p>8. Can the data be portable to different cloud provider? How long it will take to migrate to another cloud? Is there a special tool for exporting data? Yes data can be migrated but this can prove difficult if the software is proprietary and or the vendor/ supplier does not cooperate. As too how long, this depends on many factors such as the means used to transfer the data, bandwidth etc. as well as the amount to data to be transferred. Tools depend on which systems and methodology is being used.</p> <p>9. Does your cloud service provide data integrity and availability? Generally yes although this should be checked, often the public cloud has higher reliability and availability than internal cloud or data center operations, as this impacts their global business.</p> <p>10. How the original data be deleted? Is it actually erased when contract terminated.</p>
---	---

	<p>Some providers offer different levels of guarantee but it is a difficult one to be absolutely sure about, especially if you want multiple sites and back-ups to be used. You can in the end only ensure that as far as you can. It cannot always be guaranteed internally...</p> <p>11. Is it monitored? From provider to ensure acceptable use and customer</p> <p>This depends on the service and the application, if yours it is your choice to what level, if from a vendor check with them what they do but they are likely only to do from their perspective. Is the customer operating in line with any contractual agreements.</p> <p>Can the data be Non-repudiation?</p> <p>This depends on the service and application again and what you are prepared to pay. This is critical to maintain the value of digital data in archives for long-term archive storage and for criminal justice solutions.</p>
Security (Access control)	<p>12. Does the cloud provider provide management access control within sensitive data such as personal or health details?</p> <p>Access control is usually the domain of the customer organization and the VAST majority of security breaches are on the part of the organization and not the (public) cloud provider. If this is a private cloud then what is provided is down to the design of that service.</p> <p>Personal data and health data are normally protected and will have the most rigorous access controls applied.</p> <p>13. Does your cloud provider have “backdoor” for maintenance, support and services</p> <p>Again differentiate between public and private. Private cloud – that is a decision for you. Public- the provider does normally have requirements to access systems rather than data, increasingly data is encrypted with the customer holding the key, and so “backdoor” access does not imply access to data.</p> <p>Patient access to health records is becoming increasingly the norm and this is controlled by strong authentication processes.</p> <p>User/patient access control in the healthcare.</p>
Security (procedure)	<p>14. Does cloud provider provide “Auditing”</p> <p>Public cloud providers vary their terms and conditions as to what they do and don’t allow, if this is important then it would be part of your criteria when selecting a supplier.</p> <p>Certification (customer to check is it relevant to their work or not) and does it follow Personal Identifiable Information(PII) ISO/IEC 27018:2014 Not sure what this is asking?</p> <p>15. Counter measures- how does your cloud provider react about security breach?</p> <p>All vendors have their laid down procedures, and this would be for negotiation when procuring a service. But this control is one of</p>

	<p>things that differentiates on-premise from public cloud. The security challenges differ, and one of the key differences is how processes change. Incident response is a good example. If your on-premise email server gets hacked, you can go to the datacenter and unplug it. If your O365 account gets hacked, you have to contact MSFT, pass their authentication test (prove that you have the authority to take a drastic action like shutting down email), and wait for them to process the change. All that takes a lot longer. Other processes are different too – like change management. So security is different in the two environments.</p> <p>16. Testing (cloud provider what kind of security tests) The large scale providers test their services in ways that most governments cannot begin too. A recent study returned figures from cloud users saying that 61% of them believed that cloud was now at least as or MORE secure than on premise.</p> <p>But this would be for you to discuss with your chosen vendors which they may not reveal, as doing so in itself could create a security risk?</p> <p>17. If there is breach of security will the provider provide a notification to customers or not? Most if not all vendors will inform the clients of any potential or actual security breach.</p> <p>Detection Key management Security level</p>
<p>Incident management</p>	<p>18. How security incident are dealt with? Does cloud provider provide: Response? Logging? Reporting? Forensics?</p> <p>Security in the big providers is taken very seriously indeed, they will certainly investigate as a matter of course security threats. Note that companies such as Microsoft play an active role in working with police forces to identify and remove threats where possible. Security incidents will be logged and reported, the extent of any forensic examination will be based upon the seriousness of the incident and the potential threat. The issue remains that the biggest threat is from poor controls within the client organization themselves, weak access controls not enforcing policies etc. sharing of passwords etc. If you keep systems in house then these problems remain.</p> <p>For example Apple took a barrage of complaints for the celebrity photo scandal last year. “Cloud” was at fault, it was not, the fault lay with individuals who had set up weak passwords and these were compromised. Nothing to do with the underlying cloud infrastructure.</p> <p>19. Is there a certain mechanism to notify customers about data breaches or information security incident?</p>

	<p>Vendors vary in their approach and this would be one area where you may be able negotiate a better response than normal depending on your requirement.</p>
Privacy	<p>20. Non-disclosure? Can provider use or access the data? In most cases no they can neither access nor use, but examine in detail the terms and conditions issued by the vendor.</p> <p>Data minimization –Not sure to what this refers?</p>
Hybrid clouds	<p>21. Does your cloud provide rely on outsourcing some of the services? (may rely on the services from multiple provider) Hybrid cloud refers to the mix of internal private and public cloud, not generally the sub-contracting of some services. However some SaaS providers allow the customer to choose where the service may be hosted, such as on Azure or AWS or indeed a hybrid situation between the cloud and on-premise.</p> <p>Again check with your chosen provider the architecture they propose to use for any given solution or offering.</p>
Technical	<p>22. Does your cloud provider face or likely to some of the following technical issues? if yes, how it deals with?</p> <p>Resource exhaustion (under or over provisioning) Isolation failure Cloud provider malicious insider- abuse of high privilege roles Management interface compromise (manipulation, availability of infrastructure) Intercepting data in transit Insecure or ineffective deletion of data Distributed denial of service (DDoS) Economic denial of service (EDoS) Loss of Cryptographic Keys Compromise service engine Conflicts between customer hardening procedures and cloud environment</p> <p>I am unable to provide detailed answers to this list of questions and in any event the answers may vary between Vendors. But cloud is scalable and under provision is not the concern of the client, nor is over provision as you only pay for what you use.</p> <p>Data in transit is a shared responsibility with the client and encryption needs to be agreed.</p>
Legal	<p>23. Does your cloud provider clarify the status of the legal issues for instance:</p> <p>Risk from changes of jurisdiction Data protection risks Licensing risks</p> <p>They will clarify who is responsible for what and will depend on what service is being taken., For example IaaS licensing will be included up to the point of the operating system, where the client becomes responsible.</p>

	<p>24. Does cloud provider follow Health Insurance Portability and Accountability Act (HIPAA)? Microsoft Azure in the USA is accredited to HIPAA standards</p> <p>25. Does your cloud provider follow Personal Information Protection and Electronic Documents Act (PIPEDA)? You must satisfy yourself of this when choosing a provider.</p>
Risks not specific to the cloud	<p>26. Does your cloud provider face or likely to some of the following issues?</p> <ul style="list-style-type: none"> Network breaks Network management (network congestion/mis-connection/non-optimal use) Modifying network traffic Privilege escalation Social engineering attacks (impersonation) Loss or compromise of operational logs Loss or compromise of security logs (manipulation of forensic investigation) Backups lost, stolen Non Cloud-Specific Network-Related Technical Failures or Attacks Natural disasters <p>Yes of course they are subject to the same risks as everyone else, however they go to great lengths to ensure the data centers being used are not in flood plains or earthquake fault lines. But they take a great deal of effort to minimise them and are subject to the same political interference that many government agencies can be about the placing of facilities or privilege escalation etc.</p>

A.10 Interview Transcript with Undersecretary for Planning Affairs

For the purpose of this research, cloud computing is defined as “a technology model which allow patient to view his/her health records online with all resources application, software, processing power, data storage, backup facilities, development tools . Literally everything is delivered as a set of services via the Internet” (Aljabre, 2012).

Meeting main

To understand manager’s and healthcare providers attitude towards migrating healthcare services to cloud computing. It considers migrating process from management, technical, legal and security prospective. In addition, it focus on cloud security checklist any healthcare provider would like to consider before migrate their healthcare services to cloud.

Meeting Questions

Category	Question list
Role in the organization	<p>1. What are the roles you play in the healthcare organization(s)? Give more details about each role. H.Dr. Ali Talib Al Hinai Undersecretary for Planning Affairs in Ministry of Health</p>
Management perspective	<p>2.What do you think about migrating healthcare service to cloud? Ministry of health started to use cloud computing as infrastructure as a service by hosting the ministry website in cloud. The online system provides various services to patient but in different phases. For in example apply for tender or discharged summary. Also, allow patient to book and cancel appoint. But a patient cannot view his medical record online for security concerns. There is a need for organized mechanism and low for organizing viewing patient record online. In UK it is not allowed for patient to view their medical records online. In U.S it is not allowed too but in Canada patient can have access to his medical records online. Each country differ than other country according to rules and regulations. With us here in Oman, it is not allowed to view patient medical records except for authorized people. Clinical pharmacy cannot view all patient records, and administrator staff cannot view patient records. Each staff according to their roles and responsibilities. The only person can view patient medical record is the consultant if the patient under his name of treatment people. He can view the treatment plan for the patient, any surgical conducted and medication. However, the consultant cannot view the administrative work such as budget for the hospital or any financial issues.</p> <p>Given healthcare scenario about a lady from Germany went to US to attend a conference but her taxi was hit by another car and she was not unconscious in the emergency unit. The doctors prescribe a medicine she has allergic too. Luckily the doctors swap her</p>

	<p>smartphone which indicate her medical history hence, the doctors changed the medicine which could have her killed.</p> <p>Dr. Ali, there is a difference to put medical records online or to put it in cloud. The risk is too high in cloud. Using ALSHIFA system there is an internal server in ministry of health. The risk will be internal but when you put it in cloud there will be external risks from hackers from anywhere. It is fine to provide services online to book or cancel appointment even if it is hacked by someone it is not a major concern. But having patient file is top secret. If you put patient file in cloud there is a high risk of it being hacked. The cloud provides good services except for patient file.</p> <p>ALSHIFA provides different services for citizens and residents except for patient medical records. Currently, citizens and residents can use their ID card to give hospital or health center authority to view his medical record when he needs treatment. At a later stage, there will be a central database which unifies patient files in one place.</p> <p>There are two servers, one in the ministry of health and the other one in ITA as a backup. This represents a disaster recovery plan. Currently, we are working on enhancing security rules among all hospitals, but all sectors have to apply ALSHIFA systems within their sector.</p> <p>Will the codes in al Shifa a system is known internationally in different countries?</p> <p>Yes, of course the codes used within ALSHIFA are globally used.</p>
Technology importance order	<p>How would you order the following points in the technology factor according to importance?</p> <ul style="list-style-type: none"> • CIA-----5 • Complex and Cost----4 • Internet based services ---3 • Privacy----1 • Data Security ----2 • Provider Control ----6 • Business application -----7 • Social networking-----8
Challenges in 4 factors	<p>What do you think of Human challenges</p> <p>Medical teams tend to resist change and new information technology</p> <p>Technology Challenges CIA (confidentiality, integrity, availability), Complex and cost, internet based services, privacy, provider control and business applications.</p> <p>Organizational Challenges Will top management support cloud computing migration? Are there adequate resources to migrate healthcare services to cloud computing?</p>

	<p>Will the perceived benefits of utilizing cloud computing cut down operating costs in healthcare?</p> <p>Environmental Challenges Government policy</p>
--	--

12 Appendix B: Questionnaires

B.1 Questionnaire Justification

Question Statement	Justification
<p><i>Part # 1 Personal Information</i></p> <p>1.Nationality: 2.Gender: 3.Age: 4.Education Degree: 5. Designation at work:</p>	The first part seeks information about demographic data about the participant

Question Statement	Justification	Sources
<p><i>Part # 2</i></p> <p>1. Do you have IT Experience? 2. Have you ever heard of cloud computing? 3. Do you know the meaning of cloud computing? 4. Do you use cloud computing services today? 5. Do you think cloud computing is safe?</p>	Those questions seeks information about participant awareness of IT experience in general and cloud computing as service in particular and if they think it is safe to use or not.	Wijaya et al. (2014)

Question Statement	Justification	Sources
<p><i>Part # 3: Internet based Services</i></p> <p>I1.Social Networking Sites e.g. Facebook, MySpace and Friendster. I2.Professional Social Networking sites e.g. LinkedIn and Xing. I3.Online media storage e.g. Flickr and YouTube. I4.Internet-based email e.g. Gmail and Hotmail. I5.Online Office Suites e.g. GoogleDocs and Prezi. I6.Business Applications e.g. Salesforce.com, Spendvision and Insight.</p>	<p>Those questions to investigate participant knowledge and use of internet based services within their daily life and work environment on Likert scale from Use Frequently to Never heard of.</p> <p>The researcher added extra column for I do not know as an option for participant if they are not aware of the topic</p>	Wijaya et al. (2014)

I7.Platform services e.g. Google Apps Engine and Microsoft Azure.		
I8.Infrastructure services e.g. Amazon EC2 and Amazon S3.		

Question Statement	Justification	Sources
<p><i>Part # 4: Privacy</i></p> <p>P1.You believe it is fine to share your personal details (e.g name, gender, material status, date of birth, contact number, home address, e-mail) online.</p> <p>P2.You believe it is fine to share your business details (job information, business address, phone number, e-mail) online.</p> <p>P3.You believe it is fine to share your education details online</p> <p>P4.You believe it is fine to share your medical information online</p> <p>P5.You believe it is fine to share your credit card details online</p> <p>P6.You believe it is fine to share your (e.g. photo, video's) online.</p>	<p>Those questions seeks information concerning participant's perceptions of privacy in their personal details, business details, education details, medical information and credit card details online.</p> <p>It intend to know participant's perceptions of cloud security and privacy threats on Likert scale for Strongly Disagree to Strongly Agree as well as adding I do not know option.</p>	Wijaya et al. (2014)

Question Statement	Justification	Sources
<p><i>Part # 5: Human</i></p> <p>H1: Among your peers, you are among the first who try out new information technologies.</p> <p>H2: You like to experiment with new information technologies.</p> <p>H3: Employees (and patients) are enthusiastic about the cloud computing technology adoption in healthcare services.</p> <p>H4: Employees (and patients) are ready to accept the changes caused by the cloud computing technology adoption in healthcare services.</p>	<p>Those questions concerning participant's perceptions whether they are willing and ready to adopt new technology or not. Human play an important role in the successful implementation of new information technology in the delivery of healthcare services if they have a positive attitude.</p>	Lian et al., (2014)

Question Statement	Justification	Sources
<p><i>Part # 6 Technological</i></p> <p>T1: Cloud computing in Healthcare services should enforce security controls (such as the cryptographic system) to protect patient sensitive information.</p> <p>T2: In the current healthcare systems, unauthorized employees are prohibited from accessing patient's/ medical information resources.</p> <p>T3: Employees follow healthcare policy and regulations when releasing or transmitting medical information.</p> <p>T4: In the current healthcare systems, healthcare service has well implemented security practices to protect important medical information from being stolen by malicious intrusions (such as break-in, Trojans, and spy-wares).</p> <p>T5: In the current healthcare systems, information security measures are implemented in healthcare services to prevent sensitive information from unauthorized disclosure.</p> <p>T6: In the current healthcare systems, healthcare provider constantly updates information resources and regularly creates information backups.</p> <p>T7: In the current healthcare systems, healthcare provider regularly conducts risk assessment and updates security plans to reduce the probability of loss of information.</p> <p>T8: When acquiring important information from the information sources or business partners, employees will store it into the hospital's database.</p> <p>T9: Healthcare provider has security controls (such as change</p>	<p>Technological entails the internal and external influences of adopting specific information technology. Those questions seeks information concerning participant's perceptions in adopting cloud computing as services and what are the critical key factors in information security such as; confidentiality, integrity, availability, data security, complex, cost and compatibility which might influence the decision to adopt cloud computing or not.</p>	<p>Lian et al., (2014)</p>

<p>management procedures) in place to prevent unauthorized information changes (creation, alternation, and deletion).</p> <p>T10: The database is periodically reconciled and regularly maintained in hospitals to increase the accuracy and reliability of information.</p> <p>T11: Healthcare provider pays attentions to lower down the probability of information system breakdown and information service disruption.</p> <p>T12: There are well established information access control procedures in hospitals, to make sure that for any particular information resource only authenticated users with right privileges can access such resource.</p> <p>T13: In the current healthcare systems, a legitimate user with business needs can access hospital information at any time and at any place.</p> <p>T14: Cloud computing technology provides a secure channel for transferring medical data across different sites.</p> <p>T15: When using cloud-computing technology may cause your medical data to be stolen.</p> <p>T16: You do not think it is safe to use cloud-computing technology in healthcare because of security concerns.</p> <p>T17: You believe by using cloud computing in healthcare there is a significant risk of data loss.</p> <p>T18: You believe by using cloud computing in healthcare there is risk of data being misused by cloud computing provider</p> <p>T19: You believe by using cloud computing in healthcare there is risk of unauthorized data access</p>		
---	--	--

<p>T20: You believe by using cloud computing in healthcare there is risk of unauthorised data manipulation i.e. data fraud</p> <p>T21: You believe by using cloud computing in healthcare there is risk of data exposure to other users of the cloud service</p> <p>T22: You believe by using cloud computing in healthcare there is risk of losing control over data location.</p> <p>T23: You believe by using cloud computing in healthcare there is risk of data theft via external attacks such as hacking</p> <p>T24: You believe by using cloud computing in healthcare there is risk of data being accessed by government departments outside of healthcare.</p> <p>T25: The skills required to use cloud in healthcare are too complex for the most of people.</p> <p>T26: Learning to use cloud applications in healthcare is too time consuming.</p> <p>T27: It is difficult to transfer current healthcare systems to cloud computing platform.</p> <p>T28: It is complex to develop Cloud Computing applications in healthcare.</p> <p>T29: It is complex to maintain Cloud Computing platform in healthcare.</p> <p>T30: Adopting cloud technology in healthcare is compatible with current healthcare services practices.</p> <p>T31: Adopting cloud technology is compatible with hospital's core values and goals.</p> <p>T32: Adopting cloud technology is compatible with current information infrastructure in the hospitals.</p> <p>T33: The cost of establishing Cloud technology in healthcare</p>		
---	--	--

<p>services is far greater than the expected benefits.</p> <p>T34: The cost of maintaining Cloud technology in healthcare services is likely to be higher than maintaining the current system.</p> <p>T35: The cost of Cloud technology user training in healthcare services is likely to be high.</p>		
--	--	--

Question Statement	Justification	Sources
<p><i>Part # 7 : Organisational</i></p> <p>O1: Adopting cloud computing technology in healthcare services can improve the collaboration and communication between professionals involved in the patient treatment plan.</p> <p>O2: Adopting cloud computing technology in healthcare services can reduce the operating costs</p> <p>O3: Cloud computing technology can provide more timely access to patient information.</p> <p>O4: Top managers are likely to support the adoption of cloud computing technology in healthcare services.</p> <p>O5: Top managers are likely to provide sufficient resources to adopt cloud technology in healthcare services.</p> <p>O6: Top managers are likely to understand the benefits of cloud technology in healthcare services.</p> <p>O7: Top managers are likely to encourage the development of healthcare services using Cloud Computing.</p> <p>O8: Hospital have sufficient IT infrastructure to support the development of cloud computing technology in healthcare services.</p>	<p>This part for healthcare professional only as the questions seeks information concerning their perceptions in terms of what factors might affect hospital intention to adopt new information systems technology. Some variables might be relative advantage if adopting cloud computing can reduce the operating costs and increase the relative operational benefits for a given hospital, benefits for adopting cloud computing in healthcare services.</p> <p>In addition, Adequate resources; the adoption of cloud computing technology is usually a large project and a huge undertaking for hospitals. If a given hospital has a sufficient budget, adequate human resource support, ample time, and good top manager's involvement, then the adopting of cloud computing</p>	<p>Chang et al., (2007)</p> <p>Lian et al., (2014)</p> <p>Singh et al., (2014)</p>

<p>O9: Hospital have enough human resources to develop cloud computing technology in healthcare services.</p> <p>O10: Hospital have enough time to develop cloud-computing technology in healthcare services.</p> <p>O11: Hospital have enough budget to develop cloud-computing technology in healthcare services.</p> <p>O12: Adopting cloud computing technology can improve hospital image and expertise.</p> <p>O13: Adopting cloud computing technology can improve internal efficiency.</p> <p>O14: Adopting cloud computing technology can improve healthcare service quality.</p> <p>O15: Adopting cloud computing technology can improve the relationship between hospital and patient.</p> <p>O16: Adopting cloud computing technology can provide 24x7 worldwide accessibility to medical records.</p> <p>O17: Adopting cloud computing technology will reduce duplicate patient tests.</p> <p>O18: Adopting cloud computing technology can reduce time needed for doctors to access the patient treatment plan.</p> <p>O19: Adopting cloud computing technology can increase health research and collaboration between various healthcare providers.</p> <p>O20: Adopting cloud computing technology can improve the reliability of IT resources to avoid server break down or data loss.</p>	<p>technology will be met in a positive manner</p> <p>The Top management support which refers to whether or not the executives understand the nature and functions of cloud computing technology and therefore fully support the development of it.</p>	
--	---	--

Question Statement	Justification	Sources
--------------------	---------------	---------

<p><i>Part # 8 Environmental</i></p> <p>E1: Healthcare cloud computing development is a key priority for the government.</p> <p>E2: The government should develop Electronic Medical Records using cloud computing.</p> <p>E3: Training courses on how to use cloud computing technology in healthcare should be provided by the government.</p> <p>E4: High quality of training programs will be provided by the Cloud provider.</p> <p>E5: High quality of training programs will be provided by the Hospitals.</p> <p>E6: High quality of ongoing technical support will be provided by the Cloud provider.</p>	<p>This part for healthcare professional only as the questions seeks as the questions seeks information concerning healthcare professional perceptions in terms of government policies have a positive impact on hospitals trying to adopt new information systems technology or not.</p>	<p>Chang et al., (2007)</p> <p>Lian et al., (2014)</p> <p>Singh et al., (2014)</p>
--	---	--

B.2 Public Questionnaire

Questionnaire: Perception of Security using Cloud Computing in the Delivery of Healthcare Services (Public)

This questionnaire has been developed for a research purpose only and used to evaluate the Perception of Security using Cloud Computing in the delivery of Healthcare Services. The researcher is a PhD student at Cardiff University, United Kingdom. All information provided will remain strictly confidential.

Thank you for your participation and Co-operation

For the purpose of this research, cloud computing is defined as “a technology model which allow patient to view his/her health records online with all resources application, software, processing power, data storage, backup facilities, development tools . Literally everything is delivered as a set of services via the Internet” (Aljabre, 2012). I will be grateful if you could spend 20 to 30 minutes on answering the following questionnaire.

تحياتي العزيزة سيدي/ سيدتي،

انا طالبة دكتوراه في جامعه كاريف بالمملكة المتحدة وأود إجراء استبيان حول "مفهوم الامن باستخدام الحوسبة السحابية في تقديم الخدمات الصحية. لغرض هذا البحث يتم تعريف الحوسبة السحابية بأنها نموذج التكنولوجيا التي تسمح للمريض بعرض السجلات الطبية على الانترنت مع جميع تطبيقات الموارد والبرامج وقوه المعالجة وتخزين البيانات، والنسخ الاحتياطية وأدوات التنمية. بمعنى اخر يتم تسليم كل شيء على شكل مجموعه من الخدمات عبر الانترنت. سأكون ممتنه كثيرا لأتاحه 20-30 دقيقة للإجابة على الاستبيان التالي

Aim:

The aim of this questionnaire is to identify stakeholders’ perceptions of information security in the national cloud-based health record infrastructure provided by the Omani Ministry of Health. Also to understand how to attain the right balance between Confidentiality, Integrity and Availability (CIA) of medical data in a cloud-based health record.

Part 1: Personal Information

Nationality: [] Omani [] Saudi [] Emirati [] Bahraini [] Qatari [] Kuwait [] Other Specify

.....

Gender:

[] Male [] Female

Age:

- 18-22 23-30 years 31-40 years
 41-49years 50-59 years 60 years or more

Education Degree:

- High School Diploma Bachelor's Degree
 Master's Degree PhD Degree Other Specify

Designation at work:

- Employed, working full-time Not employed, Not looking for work
 Employed, working part-time Retired
 Not employed, looking for work Disabled, not able to work

Part 2:

1. Do you have IT Experience? Yes No
 هل لديك معرفه بتقنية المعلومات
2. Have you ever heard of cloud computing? Yes No
 هل سبق لك أن سمعت عن الحوسبة السحابية؟
3. Do you know the meaning of cloud computing? Yes No
 هل تعرف معنى الحوسبة السحابية
4. Do you use cloud computing services today? Yes No
 هل تستخدم خدمات الحوسبة السحابية اليوم؟
5. Do you think cloud computing is safe? Yes No
 هل تعتقد أن الحوسبة السحابية آمنة؟

Part 3: The following set of statements relates to how often you use the following **Internet-based services**. For each statement, please choose the answer that best represents your opinion “Never Heard of these” to “Use Very Frequently” and “N/A” if the statement is not applicable.

العبارات التالية تعبر عن مدى استخدامك للخدمات المستندة على الإنترنت. لكل عبارة اختر ما يناسبك من "الم لا تنطبق عليك" N/A "اسمع بها مطلقاً" و "تستخدمها بشكل متكرر جداً" و

Statement	Never heard of these	Never Used	Not Applicable	Use Rarely	Use Frequently	Use Very Frequently
I1.Social Networking Sites e.g. Facebook, MySpace and Friendster مواقع الشبكات الاجتماعية مثل الفيسبوك، ماي سبيس وفريندستر						
I2. Professional Social Networking sites e.g. LinkedIn and Xing مواقع الشبكات الاجتماعية المهنية						
I3. Online media storage e.g. Flickr and YouTube وسائط التخزين عبر الإنترنت على سبيل المثال فليكر ويوتيوب						
I4. Internet-based email e.g. Gmail and Hotmail على شبكة الإنترنت مثل البريد الإلكتروني بريد جوجل وهوتميل						
I5. Online Office Suites e.g. GoogleDocs and Prezi أون لاين أوفيس سوتس على سبيل المثال GoogleDocs and Prezi						
I6. Business Applications e.g. Salesforce.com, Spendvision and Insight Salesforce.com, تطبيقات الأعمال على سبيل المثال Spendvision						
I7. Platform services e.g. Google Apps Engine and Microsoft Azure منصة خدمات مثل تطبيقات جوجل ومحرك مايكروسوفت أזור						
I8. Infrastructure services e.g. Amazon EC2 and Amazon S3 S3 وأمازون EC2 خدمات البنية التحتية مثل أمازون						

Part 4: How do you value the **Privacy** of your information?

For each statement, please choose the answer that best represents your opinion 1 "Strongly Disagree" to 5 "Strongly Agree", "Neutral" if the statement is not applicable.

كيف تقدر خصوصية المعلومات الخاصة بك؟ لكل عبارة اختر ما يناسبك "لا أوافق بشدة" "أوافق بشدة"، "N/A". محايد" إذا كانت العبارة لا ينطبق

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
P1. You believe it is fine to share your personal details (e.g name, gender, material status, date of birth, contact number, home address, e-mail) online انت تعتقد أنه من الجيد تبادل التفاصيل الشخصية الخاصة بك (مثل الاسم والجنس والوضع المادي، وتاريخ الميلاد، رقم الاتصال، عنوان المنزل، والبريد الإلكتروني) عبر الإنترنت					
P2. You believe it is fine to share your business details (job information, business address, phone number, e-mail) online انت تعتقد أنه من الجيد تبادل التفاصيل الشخصية الخاصة بك (مثل الاسم والجنس والوضع المادي، وتاريخ الميلاد، رقم الاتصال، عنوان المنزل، والبريد الإلكتروني) عبر الإنترنت					
P3. You believe it is fine to share your education details online انت تعتقد أنه من الجيد تبادل تفاصيل التعليم الخاصة بك على الإنترنت					
P4. You believe it is fine to share your medical information online انت تعتقد أنه من الجيد تبادل المعلومات الطبية الخاصة بك على الإنترنت					
P5. You believe it is fine to share your credit card details online انت تعتقد أنه من الجيد تبادل تفاصيل بطاقة الائتمان الخاصة بك على الإنترنت					
P6. You believe it is fine to share your (e.g. photo, video's) online. انت تعتقد انه امر جيد ان تشارك (مثل الصور ومقاطع الفيديو) على الإنترنت					

Part 5: The following set of statements relates to Human Domain. For each statement, please choose the answer that best represents your opinion “Strongly Disagree” to “Strongly Agree”, “Neutral” if the statement is not applicable. “N/A” if you do not know.

فيما يلي مجموعة من العبارات تتعلق بمجال الإنسان. لكل عبارة اختر ما يناسبك "لا أوافق بشدة" "أوافق
إذا كنت لا تعرف "N / A" بشدة"، "محايد" إذا كانت العبارة لا ينطبق

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	N/A
H1: Among your peers, you are among the first who try out new information technologies. من بين زملائك، انت أول من يجرب الجديد من تكنولوجيات المعلومات.						
H2: You like to experiment with new information technologies. انت تحب ان تجرب الجديد من تكنولوجيات المعلومات						
H3: Employees (and patients) are enthusiastic about the cloud computing technology adoption in healthcare services. الموظفين (والمرضى) متحمسون لأعتماد تكنولوجيا الحوسبة السحابية في خدمات الرعاية الصحية.						
H4: Employees (and patients) are ready to accept the changes caused by the cloud computing technology adoption in healthcare services. الموظفين (والمرضى) على استعداد لقبول التغييرات الناجمة عن اعتماد تكنولوجيا الحوسبة السحابية في خدمات الرعاية الصحية.						

Part 6: The following set of statements relates to Technology Domain. For each statement, please choose the answer that best represents your opinion “Strongly Disagree” to “Strongly Agree” and “Neutral” if the statement is not applicable, “N/A” if you do not know.

المجموعة التالية من العبارات تتعلق بالمجال التقني. لكل عبارة اختر ما يناسبك "لا أوافق بشدة" "أوافق بشدة"
إذا كنت لا تعرف "N / A" و "محايد" إذا كانت العبارة لا تنطبق،

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	N/A
T1: Cloud computing in Healthcare services should enforce security controls (such as the cryptographic system) to protect patient sensitive information. الحوسبة السحابية في خدمات الرعاية الصحية يجب أن تطبق الضوابط الأمنية (مثل نظام التشفير) لحماية المعلومات الحساسة للمرضى.						
T2: In the current healthcare systems, unauthorized employees are prohibited from accessing patient's/ medical information resources. في أنظمة الرعاية الصحية الحالية، يحظر على الموظفين غير المخولين من الوصول إلى موارد المعلومات الطبية / المريض.						
T3: Employees follow healthcare policy and regulations when releasing or transmitting medical information. الموظفين يتبعون السياسات واللوائح الصحية عند الإفصاح أو نقل المعلومات الطبية.						
T4: In the current healthcare systems, healthcare service has well implemented security practices to protect important medical information from being stolen by malicious intrusions (such as break-in, Trojans, and spy-wares). في أنظمه الرعاية الصحية الحالية يوجد ممارسات امنيه لحماية المعلومات الطبية من الاختراقات الخبيثة مثل أحصنة طروادة والتجسس						
T5: In the current healthcare systems, information security measures are implemented in healthcare services to prevent sensitive information from unauthorized disclosure. في أنظمة الرعاية الصحية الحالية، يتم تنفيذ تدابير أمن المعلومات في خدمات الرعاية الصحية لمنع المعلومات الحساسة من الكشف لغير المصرح لهم						
T6: In the current healthcare systems, healthcare provider constantly updates information resources and regularly creates information backups. في أنظمة الرعاية الصحية الحالية، يقوم مزود الرعاية الصحية بتحديث موارد المعلومات باستمرار وينشئ نسخ احتياطية من المعلومات باستمرار						

<p>T7: In the current healthcare systems, healthcare provider regularly conducts risk assessment and updates security plans to reduce the probability of loss of information.</p> <p>في أنظمة الرعاية الصحية الحالية، مزود الرعاية الصحية يجري بشكل منتظم تقييم المخاطر ويحدث خطط الامن للحد من احتمال فقدان المعلومات</p>					
<p>T8: When acquiring important information from the information sources or business partners, employees will store it into the hospital's database.</p> <p>عند الحصول على معلومات مهمة من مصادر المعلومات أو الشركاء التجاريين، يقوم الموظفون بتخزينها في قاعدة البيانات بالمستشفى</p>					
<p>T9: Healthcare provider has security controls (such as change management procedures) in place to prevent unauthorized information changes (creation, alternation, and deletion).</p> <p>مزود الرعاية الصحية لديه ضوابط أمنية (مثل إجراءات إدارة التغيير) في المكان لمنع التغييرات غير المصرح بها للمعلومات (إنشاء، التناوب، وحذف).</p>					
<p>T10: The database is periodically reconciled and regularly maintained in hospitals to increase the accuracy and reliability of information.</p> <p>يتم التوفيق بين قاعدة البيانات بشكل دوري وصيانتها بانتظام في المستشفيات لزيادة دقة المعلومات وموثوقيتها</p>					
<p>T11: Healthcare provider pays attentions to lower down the probability of information system breakdown and information service disruption.</p> <p>مزود الرعاية الصحية يولي انتباه شديد لخفض احتمال انهيار نظام المعلومات وانقطاع خدمة المعلومات</p>					
<p>T12: There are well established information access control procedures in hospitals, to make sure that for any particular information resource only authenticated users with right privileges can access such resource.</p> <p>توجد إجراءات مراقبة الوصول إلى المعلومات في المستشفيات، للتأكد من أن أي مصدر معلومات خاص لا يمكن إلا المستخدمين المصادق عليهم مع امتيازات حق الوصول إلى هذه الموارد</p>					

T13: In the current healthcare systems, a legitimate user with business needs can access hospital information at any time and at any place. في أنظمة الرعاية الصحية الحالية، يمكن للمستخدم الشرعي (أو المخول) مع احتياجات العمل الوصول لمعلومات المستشفى في أي وقت وفي أي مكان.						
T14: Cloud computing technology provides a secure channel for transferring medical data across different sites. توفر سحابة تقنيات الحوسبة قناة آمنة لنقل البيانات الطبية عبر مواقع مختلفة.						
T15: When using cloud-computing technology may cause your medical data to be stolen. عند استخدام تقنية الحوسبة السحابية قد يؤدي الى سرقة البيانات الطبية الخاصة بك						
T16: You do not think it is safe to use cloud-computing technology in healthcare because of security concerns. انت لا تعتقد أن استخدام تكنولوجيا الحوسبة السحابية في مجال الرعاية الصحية امن بسبب مخاوف أمنية						
T17: You believe by using cloud computing in healthcare there is a significant risk of data loss. انت تعتقد باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر كبير من فقدان البيانات						
T18: You believe by using cloud computing in healthcare there is risk of data being misused by cloud computing provider انت تعتقد باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر من البيانات التي يساء استخدامها من قبل مزود الحوسبة السحابية						
T19: You believe by using cloud computing in healthcare there is risk of unauthorized data access أنت تؤمن باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر من الوصول إلى البيانات من قبل غير المصرح لهم						
T20: You believe by using cloud computing in healthcare there is risk of unauthorised data manipulation i.e. data fraud أنت تؤمن باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر التلاعب وتزوير البيانات من غير المصرح لهم						

T21: You believe by using cloud computing in healthcare there is risk of data exposure to other users of the cloud service أنت تؤمن باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر كشف البيانات للمستخدمين الآخرين للخدمة السحابية						
T22: You believe by using cloud computing in healthcare there is risk of losing control over data location. انت تعتقد باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر فقدان السيطرة على موقع البيانات						
T23: You believe by using cloud computing in healthcare there is risk of data theft via external attacks such as hacking أنت تؤمن باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر سرقة البيانات عن طريق الهجمات الخارجية مثل القرصنة						
T24: You believe by using cloud computing in healthcare there is risk of data being accessed by government departments outside of healthcare. انت تعتقد باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر وصول البيانات لدوائر حكومية خارج الرعاية الصحية						
T25: The skills required to use cloud in healthcare are too complex for the most of people. المهارات اللازمة لاستخدام الحوسبة السحابية في مجال الرعاية الصحية معقدة للغاية بالنسبة لمعظم الأشخاص						
T26: Learning to use cloud applications in healthcare is too time consuming. تعلم كيفية استخدام التطبيقات السحابية في مجال الرعاية الصحية تأخذ وقتاً أطول من اللازم						
T27: It is difficult to transfer current healthcare systems to cloud computing platform. من الصعب نقل أنظمة الرعاية الصحية الحالية إلى منصة الحوسبة السحابية						
T28: It is complex to develop Cloud Computing applications in healthcare. من المعقد تطوير تطبيقات الحوسبة السحابية في مجال الرعاية الصحية						
T29: It is complex to maintain Cloud Computing platform in healthcare. من المعقد الإبقاء على منصة الحوسبة السحابية في مجال الرعاية الصحية						

T30: Adopting cloud technology in healthcare is compatible with current healthcare services practices. اعتماد التكنولوجيا السحابية في مجال الرعاية الصحية متوافق مع ممارسات خدمات الرعاية الصحية الحالية.						
T31: Adopting cloud technology is compatible with hospital's core values and goals. اعتماد التكنولوجيا السحابية متوافق مع القيم الأساسية لأهداف المستشفى						
T32: Adopting cloud technology is compatible with current information infrastructure in the hospitals. اعتماد التكنولوجيا السحابية متوافق مع البنية التحتية للمعلومات الحالية في المستشفيات						
T33: The cost of establishing Cloud technology in healthcare services is far greater than the expected benefits إن تكلفة إنشاء التكنولوجيا السحابية في خدمات الرعاية الصحية هي أكبر بكثير من الفوائد المتوقعة						
T34: The cost of maintaining Cloud technology in healthcare services is likely to be higher than maintaining the current system. تكلفة الحفاظ على التكنولوجيا السحابية في خدمات الرعاية الصحية من المرجح أن تكون أعلى من الحفاظ على النظام الحالي.						
T35: The cost of Cloud technology user training in healthcare services is likely to be high. تكلفة تدريب المستخدمين لتكنولوجيا الحوسبة السحابية في خدمات الرعاية الصحية من المرجح أن تكون مرتفعة						

B.3 Healthcare Professionals Questionnaire

Questionnaire: Perception of Security using Cloud Computing in the Delivery of Healthcare Services (Healthcare Professional)

This questionnaire has been developed for a research purpose only and used to evaluate the Perception of Security using Cloud Computing in the delivery of Healthcare Services . The researcher is a PhD student at Cardiff University, United Kingdom. All information provided will remain strictly confidential.

Thank you for your participation and Co-operation

For the purpose of this research, cloud computing is defined as “a technology model which allow patient to view his/her health records online with all resources application, software, processing power, data storage, backup facilities, development tools . Literally everything is delivered as a set of services via the Internet” (Aljabre, 2012). I will be grateful if you could spend 20 to 30 minutes on answering the following questionnaire.

تحياتي العزيزة سيدي/ سيدتي،

انا طالبه دكتوراه في جامعه كاريف بالمملكة المتحدة وأود إجراء استبيان حول "مفهوم الامن باستخدام الحوسبة السحابية في تقديم الخدمات الصحية. لغرض هذا البحث يتم تعريف الحوسبة السحابية بأنها نموذج التكنولوجيا التي تسمح للمريض بعرض السجلات الطبية على الانترنت مع جميع تطبيقات الموارد والبرامج وقوه المعالجة وتخزين البيانات، والنسخ الاحتياطية وأدوات التنمية. بمعنى اخر يتم تسليم كل شيء على شكل مجموعه من الخدمات عبر الانترنت. سأكون ممتنه كثيرا لأتاحه 20-30 دقيقة للإجابة على الاستبيان التالي

Aim:

The aim of this questionnaire is to identify stakeholders' perceptions of information security in the national cloud-based health record infrastructure. Also to understand how to attain the right balance between Confidentiality, Integrity and Availability (CIA) of medical data in a cloud-based health record.

الهدف من الاستبيان هو معرفه الراي العام لتصور امن المعلومات باستخدام الحوسبة السحابية في تقديم الخدمات الصحية وأيضاً تحقيق التوازن بين سرية المعلومات وتوافر البيانات الطبية ومصداقيتها عبر الحوسبة السحابية

Part 1: Personal Information

Nationality: Omani Saudi Emirati Bahraini
 Qatari Kuwait Other Specify

Gender:

Male Female

Age:

- 18-22 23-30 years 31-40 years
 41-49years 50-59 years 60 years or more

Education Degree:

- High School Diploma Bachelor's Degree
 Master's Degree PhD Degree Other Specify.....

Designation at work:

- Medical Doctor Administrator Assistant Director
 Healthcare Manager Nurse Student
 Pharmacist Retired Healthcare IT Support
 Assistant Pharmacist Other Please Specify:

Part 2:

1. Do you have IT Experience? Yes No
هل لديك معرفه بتقنية المعلومات
2. Have you ever heard of cloud computing? Yes No
هل سبق لك أن سمعت عن الحوسبة السحابية؟
3. Do you know the meaning of cloud computing? Yes No
هل تعرف معنى الحوسبة السحابية
4. Do you use cloud computing services today? Yes No
هل تستخدم خدمات الحوسبة السحابية اليوم؟
5. Do you think cloud computing is safe? Yes No
هل تعتقد أن الحوسبة السحابية آمنة؟

Part 3: The following set of statements relates to how often you use the following **Internet-based services**. For each statement, please choose the answer that best represents your opinion “Never Heard of these” to “Use Very Frequently” and “N/A” if the statement is not applicable.

العبارات التالية تعبر عن مدى استخدامك للخدمات المستندة على الانترنت. لكل عبارة اختر ما يناسبك من "الم لا تنطبق عليك " N/A " اسمع بها مطلقا" و " تستخدمها بشكل متكرر جداً" و

Statement	Never heard of these	Never Used	Not Applicable	Use Rarely	Use Frequently	Use Very Frequently
I1.Social Networking Sites e.g. Facebook, MySpace and Friendster مواقع الشبكات الاجتماعية مثل الفيسبوك، ماي سبيس وفرييندستر						
I2.Professional Social Networking sites e.g. LinkedIn and Xing مواقع الشبكات الاجتماعية المهنية						
I3.Online media storage e.g. Flickr and YouTube وسائط التخزين عبر الإنترنت على سبيل المثال فليكر ويوتيوب						
I4.Internet-based email e.g. Gmail and Hotmail على شبكة الإنترنت مثل البريد الإلكتروني بريد جوجل وهوتميل						
I5.Online Office Suites e.g. GoogleDocs and Prezi أون لاين أوفيس سوتس على سبيل المثال GoogleDocs and Prezi						
I6.Business Applications e.g. Salesforce.com, Spendvision and Insight تطبيقات الأعمال على سبيل المثال Salesforce.com, Spendvision						
I7.Platform services e.g. Google Apps Engine and Microsoft Azure منصة خدمات مثل تطبيقات جوجل ومحرك مايكروسوفت أزور						
I8.Infrastructure services e.g. Amazon EC2 and Amazon S3 وأمازون EC2 خدمات البنية التحتية مثل أمازون S3						

Part 4: How do you value the **Privacy** of your information?

For each statement, please choose the answer that best represents your opinion “Strongly Disagree” to “Strongly Agree”, “Neutral” if the statement is not applicable.

كيف تقدر خصوصية المعلومات الخاصة بك؟ لكل عبارة اختر ما يناسبك "لا أوافق بشدة" "أوافق بشدة"،
N/A. "محايد" إذا كانت العبارة لا ينطبق

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
P1. You believe it is fine to share your personal details (e.g name, gender, material status, date of birth, contact number, home address, e-mail) online انت تعتقد أنه من الجيد تبادل التفاصيل الشخصية الخاصة بك (مثل الاسم والجنس والوضع المادي، وتاريخ الميلاد، رقم الاتصال، عنوان المنزل، والبريد الإلكتروني) عبر الإنترنت					
P2. You believe it is fine to share your business details (job information, business address, phone number, e-mail) online انت تعتقد أنه من الجيد تبادل التفاصيل الشخصية الخاصة بك (مثل الاسم والجنس والوضع المادي، وتاريخ الميلاد، رقم الاتصال، عنوان المنزل، والبريد الإلكتروني) عبر الإنترنت					
P3. You believe it is fine to share your education details online انت تعتقد أنه من الجيد تبادل تفاصيل التعليم الخاصة بك على الإنترنت					
P4. You believe it is fine to share your medical information online انت تعتقد أنه من الجيد تبادل المعلومات الطبية الخاصة بك على الإنترنت					
P5. You believe it is fine to share your credit card details online انت تعتقد أنه من الجيد تبادل تفاصيل بطاقة الائتمان الخاصة بك على الإنترنت					
P6. You believe it is fine to share your (e.g. photo, video's) online. انت تعتقد أنه من الجيد ان تشارك (مثل الصور ومقاطع الفيديو) على الإنترنت.					

Part 5 :The following set of statements relates to Human Domain. For each statement, please choose the answer that best represents your opinion “Strongly Disagree” to “Strongly Agree”, “Neutral” if the statement is not applicable. “ N/A” if you do not know.

فيما يلي مجموعة من العبارات تتعلق بمجال الإنسان. لكل عبارة اختر ما يناسبك "لا أوافق بشدة" "أوافق". إذا كنت لا تعرف "N / A"، "محايد" إذا كانت العبارة لا ينطبق.

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	N/A
T1: Cloud computing in Healthcare services should enforce security controls (such as the cryptographic system) to protect patient sensitive information. الحوسبة السحابية في خدمات الرعاية الصحية يجب أن تطبق الضوابط الأمنية (مثل نظام التشفير) لحماية المعلومات الحساسة للمرضى.						
T2: In the current healthcare systems, unauthorized employees are prohibited from accessing patient's/ medical information resources. في أنظمة الرعاية الصحية الحالية، يحظر على الموظفين غير المخولين من الوصول إلى موارد المعلومات الطبية / المريض.						
T3: Employees follow healthcare policy and regulations when releasing or transmitting medical information. الموظفين يتبعون السياسات واللوائح الصحية عند الإفصاح أو نقل المعلومات الطبية.						
T4: In the current healthcare systems, healthcare service has well implemented security practices to protect important medical information from being stolen by malicious intrusions (such as break-in, Trojans, and spy-wares). في أنظمه الرعاية الصحية الحالية يوجد ممارسات امنيه لحمايه المعلومات الطبيه من الاختراقات الخبيثة مثل أحصنة طروادة والتجسس						
T5: In the current healthcare systems, information security measures are implemented in healthcare services to prevent sensitive information from unauthorized disclosure. في أنظمة الرعاية الصحية الحالية، يتم تنفيذ تدابير أمن المعلومات في خدمات الرعاية الصحية لمنع المعلومات الحساسة من الكشف لغير المصرح لهم						
T6: In the current healthcare systems, healthcare provider constantly updates information resources and regularly creates information backups. في أنظمة الرعاية الصحية الحالية، يقوم مزود الرعاية الصحية بتحديث موارد المعلومات باستمرار وينشئ نسخ احتياطية من المعلومات باستمرار						

<p>T7: In the current healthcare systems, healthcare provider regularly conducts risk assessment and updates security plans to reduce the probability of loss of information.</p> <p>في أنظمة الرعاية الصحية الحالية، مزود الرعاية الصحية يجري بشكل منتظم تقييم المخاطر و يحدث خطط الامن للحد من احتمال فقدان المعلومات</p>					
<p>T8: When acquiring important information from the information sources or business partners, employees will store it into the hospital's database.</p> <p>عند الحصول على معلومات مهمة من مصادر المعلومات أو الشركاء التجاريين، يقوم الموظفون بتخزينها في قاعدة البيانات بالمستشفى</p>					
<p>T9: Healthcare provider has security controls (such as change management procedures) in place to prevent unauthorized information changes (creation, alternation, and deletion).</p> <p>مزود الرعاية الصحية لديه ضوابط أمنية (مثل إجراءات إدارة التغيير) في المكان لمنع التغييرات غير المصرح بها للمعلومات (إنشاء، التناوب، وحذف).</p>					
<p>T10: The database is periodically reconciled and regularly maintained in hospitals to increase the accuracy and reliability of information.</p> <p>يتم التوفيق بين قاعدة البيانات بشكل دوري وصيانتها بانتظام في المستشفيات لزيادة دقة المعلومات وموثوقيتها</p>					
<p>T11: Healthcare provider pays attentions to lower down the probability of information system breakdown and information service disruption.</p> <p>مزود الرعاية الصحية يولي انتباه شديد لخفض احتمال انهيار نظام المعلومات وانقطاع خدمة المعلومات</p>					
<p>T12: There are well established information access control procedures in hospitals, to make sure that for any particular information resource only authenticated users with right privileges can access such resource.</p> <p>توجد إجراءات مراقبة الوصول إلى المعلومات في المستشفيات، للتأكد من أن أي مصدر معلومات خاص لا يمكن إلا المستخدمين المصادق عليهم مع امتيازات حق الوصول إلى هذه الموارد</p>					

<p>T13: In the current healthcare systems, a legitimate user with business needs can access hospital information at any time and at any place.</p> <p>في أنظمة الرعاية الصحية الحالية، يمكن للمستخدم الشرعي (أو المخول) مع احتياجات العمل الولوج لمعلومات المستشفى في أي وقت وفي أي مكان.</p>						
<p>T14: Cloud computing technology provides a secure channel for transferring medical data across different sites.</p> <p>توفر سحابة تقنيات الحوسبة قناة آمنة لنقل البيانات الطبية عبر مواقع مختلفة.</p>						
<p>T15: When using cloud-computing technology may cause your medical data to be stolen.</p> <p>عند استخدام تقنية الحوسبة السحابية قد يؤدي الى سرقة البيانات الطبية الخاصة بك</p>						
<p>T16: You do not think it is safe to use cloud-computing technology in healthcare because of security concerns.</p> <p>انت لا تعتقد أن استخدام تكنولوجيا الحوسبة السحابية في مجال الرعاية الصحية امن بسبب مخاوف أمنية</p>						
<p>T17: You believe by using cloud computing in healthcare there is a significant risk of data loss.</p> <p>انت تعتقد باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر كبير من فقدان البيانات</p>						
<p>T18: You believe by using cloud computing in healthcare there is risk of data being misused by cloud computing provider</p> <p>انت تعتقد باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر من البيانات التي يساء استخدامها من قبل مزود الحوسبة السحابية</p>						
<p>T19: You believe by using cloud computing in healthcare there is risk of unauthorized data access</p> <p>أنت تؤمن باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر من الوصول إلى البيانات من قبل غير المصرح لهم</p>						
<p>T20: You believe by using cloud computing in healthcare there is risk of unauthorised data manipulation i.e. data fraud</p> <p>أنت تؤمن باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر التلاعب وتزوير البيانات من غير المصرح لهم</p>						

T21: You believe by using cloud computing in healthcare there is risk of data exposure to other users of the cloud service أنت تؤمن باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر كشف البيانات للمستخدمين الآخرين للخدمة السحابية						
T22: You believe by using cloud computing in healthcare there is risk of losing control over data location. انت تعتقد باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر فقدان السيطرة على موقع البيانات						
T23: You believe by using cloud computing in healthcare there is risk of data theft via external attacks such as hacking أنت تؤمن باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر سرقة البيانات عن طريق الهجمات الخارجية مثل القرصنة						
T24: You believe by using cloud computing in healthcare there is risk of data being accessed by government departments outside of healthcare. انت تعتقد باستخدام الحوسبة السحابية في مجال الرعاية الصحية هناك خطر وصول البيانات لدوائر حكومية خارج الرعاية الصحية						
T25: The skills required to use cloud in healthcare are too complex for the most of people. المهارات اللازمة لاستخدام الحوسبة السحابية في مجال الرعاية الصحية معقدة للغاية بالنسبة لمعظم الأشخاص						
T26: Learning to use cloud applications in healthcare is too time consuming. تعلم كيفية استخدام التطبيقات السحابية في مجال الرعاية الصحية تأخذ وقتاً أطول من اللازم						
T27: It is difficult to transfer current healthcare systems to cloud computing platform. من الصعب نقل أنظمة الرعاية الصحية الحالية إلى منصة الحوسبة السحابية						
T28: It is complex to develop Cloud Computing applications in healthcare. من المعقد تطوير تطبيقات الحوسبة السحابية في مجال الرعاية الصحية						
T29: It is complex to maintain Cloud Computing platform in healthcare. من المعقد الإبقاء على منصة الحوسبة السحابية في مجال الرعاية الصحية						

T30: Adopting cloud technology in healthcare is compatible with current healthcare services practices. اعتماد التكنولوجيا السحابية في مجال الرعاية الصحية متوافق مع ممارسات خدمات الرعاية الصحية الحالية.						
T31: Adopting cloud technology is compatible with hospital's core values and goals. اعتماد التكنولوجيا السحابية متوافق مع القيم الأساسية لأهداف المستشفى						
T32: Adopting cloud technology is compatible with current information infrastructure in the hospitals. اعتماد التكنولوجيا السحابية متوافق مع البنية التحتية للمعلومات الحالية في المستشفيات						
T33: The cost of establishing Cloud technology in healthcare services is far greater than the expected benefits إن تكلفة إنشاء التكنولوجيا السحابية في خدمات الرعاية الصحية هي أكبر بكثير من الفوائد المتوقعة						
T34: The cost of maintaining Cloud technology in healthcare services is likely to be higher than maintaining the current system. تكلفة الحفاظ على التكنولوجيا السحابية في خدمات الرعاية الصحية من المرجح أن تكون أعلى من الحفاظ على النظام الحالي.						
T35: The cost of Cloud technology user training in healthcare services is likely to be high. تكلفة تدريب المستخدمين لتكنولوجيا الحوسبة السحابية في خدمات الرعاية الصحية من المرجح أن تكون مرتفعة						

Part 7: The following set of statements relates to Organization Domain. For each statement, please choose the answer that best represents your opinion “Strongly Disagree” to “Strongly Agree” and “Neutral” if the statement is not applicable

المجموعة التالية من العبارات تتعلق بمجال المؤسسة او المستشفى. لكل عبارة اختر ما يناسبك "لا أوافق بشدة" "بشدة أوافق" و "محايد" إذا كانت العبارة لا تنطبق

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
O1: Adopting cloud computing technology in healthcare services can improve the collaboration and communication between professionals involved in the patient treatment plan. اعتماد تكنولوجيا الحوسبة السحابية في خدمات الرعاية الصحية قد يساعد على تحسين التعاون والتواصل بين المهنيين العاملين في خطة العلاج للمرضى.					
O2: Adopting cloud computing technology in healthcare services can reduce the operating costs. اعتماد تكنولوجيا الحوسبة السحابية في خدمات الرعاية الصحية يمكن أن تقلل من تكاليف التشغيل.					
O3: Cloud computing technology can provide more timely access to patient information. تكنولوجيا الحوسبة السحابية يمكن أن توفر الوصول إلى المعلومات الطبية للمرضى بزمان قياسي.					
O4: Top managers are likely to support the adoption of cloud computing technology in healthcare services. من المرجح أن يدعم المدراء اعتماد تكنولوجيا الحوسبة السحابية في خدمات الرعاية الصحية.					
O5: Top managers are likely to provide sufficient resources to adopt cloud technology in healthcare services. من المرجح أن يوفر المدراء الموارد الكافية لتبني تكنولوجيا الحوسبة السحابية في خدمات الرعاية الصحية.					
O6: Top managers are likely to understand the benefits of cloud technology in healthcare services. من المرجح أن يتفهم المدراء فوائد تكنولوجيا الحوسبة السحابية في خدمات الرعاية الصحية.					
O7: Top managers are likely to encourage the development of healthcare services using Cloud Computing. من المرجح أن يشجع المدراء على تطوير خدمات الرعاية الصحية باستخدام تكنولوجيا الحوسبة السحابية.					
O8: Hospital have sufficient IT infrastructure to support the development of cloud computing technology in healthcare services. المستشفى لديه البنية التحتية التقنيه الكافية لدعم تطوير تكنولوجيا الحوسبة السحابية في خدمات الرعاية الصحية.					
O9: Hospital have enough human resources to develop cloud computing technology in healthcare services. المستشفى لديه ما يكفي من الموارد البشرية لتطوير تكنولوجيا الحوسبة السحابية في خدمات الرعاية الصحية.					

O10: Hospital have enough time to develop cloud-computing technology in healthcare services. المستشفى لديه ما يكفي من الوقت لتطوير تكنولوجيا الحوسبة السحابية في خدمات الرعاية الصحية .					
O11: Hospital have enough budget to develop cloud-computing technology in healthcare services. المستشفى لديه ما يكفي من الميزانية لتطوير تكنولوجيا الحوسبة السحابية في خدمات الرعاية الصحية.					
O12: Adopting cloud computing technology can improve hospital image and expertise. اعتماد تكنولوجيا الحوسبة السحابية قد يساعد على تحسين صورة المستشفى وخبراته .					
O13: Adopting cloud computing technology can improve internal efficiency. اعتماد تكنولوجيا الحوسبة السحابية قد يساعد على تحسين الكفاءة الداخلية.					
O14: Adopting cloud computing technology can improve healthcare service quality. اعتماد تكنولوجيا الحوسبة السحابية قد يحسن جودة خدمات الرعاية الصحية.					
O15: Adopting cloud computing technology can improve the relationship between hospital and patient. اعتماد تكنولوجيا الحوسبة السحابية قد يساعد على تحسين العلاقة بين المستشفى والمريض.					
O16: Adopting cloud computing technology can provide 24x7 worldwide accessibility to medical records. اعتماد تكنولوجيا الحوسبة السحابية تتيح الوصول إلى السجلات الطبية في جميع أنحاء العالم على مدار الساعة					
O17: Adopting cloud computing technology will reduce duplicate patient tests. اعتماد تكنولوجيا الحوسبة السحابية سوف يقلل من تكرار الاختبارات للمرضى.					
O18: Adopting cloud computing technology can reduce time needed for doctors to access the patient treatment plan. اعتماد تكنولوجيا الحوسبة السحابية يمكن أن تقلل من الوقت اللازم للأطباء للوصول إلى خطة العلاجية للمرضى.					
O19: Adopting cloud computing technology can increase health research and collaboration between various healthcare providers. اعتماد تكنولوجيا الحوسبة السحابية يمكن أن تزيد البحوث الصحية والتعاون بين مختلف مقدمي الرعاية الصحية.					

O20: Adopting cloud computing technology can improve the reliability of IT resources to avoid server break down or data loss. اعتماد تقنية الحوسبة السحابية قد يحسن من موثوقية موارد تكنولوجيا المعلومات لتجنب انقطاع الخدمه أو فقدان البيانات					
---	--	--	--	--	--

Part 8: The following set of statements relates to Environment Domain. For each statement, please choose the answer that best represents your opinion “Strongly Disagree” to “Strongly Agree” and “Neutral” if the statement is not applicable.

المجموعة التالية من العبارات تتعلق بمجال البيئة. لكل عبارة اختر ما يناسبك "لا أوافق بشدة" "بشدة أوافق" و "محايد" إذا كانت العبارة لا تنطبق.

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
E1: Healthcare cloud computing development is a key priority for the government. تطوير الرعاية الصحية عن طريق الحوسبة السحابية هي أولوية رئيسية للحكومة					
E2: The government should develop Electronic Medical Records using cloud computing. على الحكومة أن تضع السجلات الطبية الإلكترونية باستخدام الحوسبة السحابية					
E3: Training courses on how to use cloud computing technology in healthcare should be provided by the government. ينبغي توفير دورات تدريبية على كيفية استخدام تكنولوجيا الحوسبة السحابية في مجال الرعاية الصحية من قبل الحكومة					
E4: High quality of training programs will be provided by the Cloud provider. سيتم توفير نوعية عالية من البرامج التدريبية من قبل مزود الحوسبة السحابية					
E5: High quality of training programs will be provided by the Hospitals. سيتم توفير نوعية عالية من البرامج التدريبية من قبل المستشفيات					
E6: High quality of ongoing technical support will be provided by the Cloud provider. سيتم توفير جودة عالية من الدعم الفني المستمر من قبل مزود الحوسبة السحابية					

B.4 Authorisation Letter from SQU

Sultan Qaboos University

OFFICE OF THE ADVISOR
FOR ACADEMIC AFFAIRS



جامعة السلطان قابوس

مكتب المستشار
للشؤون الأكاديمية

31st January 2016

TO WHOM IT MAY CONCERN

This is to certify that the University has no objection of Ms. Aseela Nasser Al Harthi, a PhD student at Cardiff University, U.K, distributing the attached questionnaire for her research titled:

“Perception of Security using Cloud Computing in the Delivery of Healthcare Services (Healthcare Professional)”

Kindly cooperate with her to obtain the data required for the research.

Prof. Taher Ba-Omar
VC's Advisor, Academic Affairs



B.5: Demographic Data of Respondent

Frequency Table

		Response type			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Professional	151	27.6	27.6	27.6
	Public	397	72.4	72.4	100.0
	Total	548	100.0	100.0	

		Nationality :			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Omani	406	74.1	74.4	74.4
	Saudi	41	7.5	7.5	81.9
	Emirati	10	1.8	1.8	83.7
	Bahraini	50	9.1	9.2	92.9
	Qatari	6	1.1	1.1	94.0
	Kuwait	7	1.3	1.3	95.2
	Other Please Specify	26	4.7	4.8	100.0
	Total	546	99.6	100.0	
Missing	System	2	.4		
Total		548	100.0		

		Gender:			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	365	66.6	67.0	67.0
	Male	180	32.8	33.0	100.0
	Total	545	99.5	100.0	
Missing	System	3	.5		
Total		548	100.0		

		Age:	
		Frequency	Percent
Missing	System	548	100.0

Education Degree

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High School	37	6.8	6.8	6.8
	Diploma	84	15.3	15.4	22.2
	Bachelor's Degree	238	43.4	43.6	65.8
	Master Degree	147	26.8	26.9	92.7
	PhD Degree	33	6.0	6.0	98.7
	Other Please Specify	7	1.3	1.3	100.0
	Total	546	99.6	100.0	
Missing	System	2	.4		
Total		548	100.0		

Designation at work:

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Employed, working full-time	216	39.4	39.9	39.9
	Employed, working part-time	25	4.6	4.6	44.5
	Not employed, looking for job	29	5.3	5.4	49.8
	Not employed, Not looking for job	22	4.0	4.1	53.9
	Retired	6	1.1	1.1	55.0
	Disabled not able to work	1	.2	.2	55.2
	Student	93	17.0	17.2	72.3
	Medical Doctor	27	4.9	5.0	77.3
	Healthcare Manager	11	2.0	2.0	79.3
	Pharmacist	29	5.3	5.4	84.7
	Assistant Pharmacist	5	.9	.9	85.6
	Administrator	17	3.1	3.1	88.7
	Nurse	33	6.0	6.1	94.8
	Assistant Director	5	.9	.9	95.8
	Staff	4	.7	.7	96.5
	Healthcare IT Support	19	3.5	3.5	100.0
	Total	542	98.9	100.0	
Missing	System	6	1.1		
Total		548	100.0		

B.6: Rotated Component Matrix^a for Public and Healthcare Professional

Rotated Component Matrix^a

	Component									
	Data Security	CIA	Complex & Cost	Internet Based Services	Privacy	Business Network	Social Network	Human	Compatible	Cloud Provider
T14	.595									
T15	.739									
T16	.730									
T17	.809									
T18	.841									
T19	.867									
T20	.862									
T21	.777									
T22	.796									
T23	.806									
T24	.644									
T3		.592								
T4		.670								
T5		.766								
T6		.750								
T7		.753								
T8		.838								
T9		.788								
T10		.797								
T11		.741								
T12		.630								
T25			.635							
T26			.636							
T27			.611							
T28			.638							
T29			.556							
T33			.652							
T34			.657							
T35			.654							
I4				.626						
I5				.598						
I7				.713						
P4				.658						
P1					.791					
P2					.813					
P3					.564					

P5					.652					
I6						.734				
I8						.735				
I1							.687			
I2							.609			
H2								0.725		
H3								0.650		
T30									.502	
T32									.653	
T1										0.610
T2										0.628

Extraction Method: Principal Component Analysis.
 Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 101 iterations.

B.7: Rotated Component Matrix for Healthcare Professional

Rotated Component Matrix^a

No		Component				
		Benefits	Gov. Policy	Adequate resource	Top Managers Support	Relative advantage
1	O12	.783				
2	O13	.739				
3	O14	.825				
4	O15	.813				
5	O16	.742				
6	O17	.788				
7	O18	.832				
8	O19	.789				
9	O20	.701				
10	E1		.628			
11	E4		.710			
12	E5		.746			
13	E6		.773			
14	O8			.563		
15	O9			.636		
16	O10			.561		
17	O11			.507		
18	O4				.708	
19	O5				.766	
20	O6				.785	
21	O7				.765	
22	O1					.810
23	O2					.811
24	O3					.818

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 10 iterations.

B.8: Radar Charts Tables

Public and Healthcare Professional

Data Security	Public % Agree	Professional % Agree	Public % Disagree	Professional % Disagree
T14: Cloud computing technology provides a secure channel for transferring medical data across different sites.	56	69	14	12
T15: When using cloud-computing technology may cause your medical data to be stolen.	50	45	23	30
T16: You do not think it is safe to use cloud-computing technology in healthcare because of security concerns.	43	44	29	26
T17: You believe by using cloud computing in healthcare there is a significant risk of data loss.	45	44	32	27
T18: You believe by using cloud computing in healthcare there is risk of data being misused by cloud computing provider	53	59	19	22
T19: You believe by using cloud computing in healthcare there is risk of unauthorized data access	65	62	18	21
T20: You believe by using cloud computing in healthcare there is risk of unauthorised data manipulation i.e. data fraud	60	51	20	27
T21: You believe by using cloud computing in healthcare there is risk of data exposure to other users of the cloud service	61	57	19	24
T22: You believe by using cloud computing in healthcare there is risk of losing control over data location.	55	53	21	29
T23: You believe by using cloud computing in healthcare there is risk of data theft via external attacks such as hacking	68	61	11	16
T24: You believe by using cloud computing in healthcare there is risk of data being accessed by government departments outside of healthcare.	60	55	23	25

Confidentiality, Integrity, Availability	Public % Agree	Professional % Agree	Public % Disagree	Professional % Disagree
T3: Employees follow healthcare policy and regulations when releasing or transmitting medical information.	72	70	9	15
T4: In the current healthcare systems, healthcare service has well implemented security practices to protect important medical information from being stolen by malicious intrusions (such as break-in, Trojans, and spy-wares).	63	69	14	15
T5: In the current healthcare systems, information security measures are implemented in healthcare services to prevent sensitive information from unauthorized disclosure.	65	64	13	20
T6: In the current healthcare systems, healthcare provider constantly updates information resources and regularly creates information backups.	65	63	8	13
T7: In the current healthcare systems, healthcare provider regularly conducts risk assessment and updates security plans to reduce the probability of loss of information.	63	60	12	21
T8: When acquiring important information from the information sources or business partners, employees will store it into the hospital's database.	68	63	5	14
T9: Healthcare provider has security controls (such as change management procedures) in place to prevent unauthorized information changes (creation, alternation, and deletion).	66	70	8	11
T10: The database is periodically reconciled and regularly maintained in hospitals to increase the accuracy and reliability of information.	69	75	8	9
T11: Healthcare provider pays attentions to lower down the probability of information	66	73	9	12

system breakdown and information service disruption.				
T12: There are well established information access control procedures in hospitals, to make sure that for any particular information resource only authenticated users with right privileges can access such resource.	69	66	9	12

Complex and Cost	Public % agree	Professional % Agree	Public % Disagree	Professional % Disagree
T25: Skills complex to use CC	39	43	38	33
T26: Learning CC time consuming	27	29	52	40
T27: Difficult to transfer Healthcare to CC.	23	27	49	50
T28: Complex to develop CC in healthcare.	21	31	54	45
T32: CC compatible with current infrastructure	47	55	14	19
T33: Cost effectiveness greater than benefits	30	26	48	40
T34: cost of maintaining CC in healthcare	41	52	34	21

Privacy	Public % Agree	Professional % Agree	Public % Disagree	Professional % Disagree
P1. You believe it is fine to share your personal details (e.g name, gender, marital status, date of birth, contact number, home address, e-mail) online	13	11	67	73
P2. You believe it is fine to share your business details (job information, business address, phone number, e-mail) online	25	22	53	53
P3. You believe it is fine to share your education details online	50	46	22	29
P4. You believe it is fine to share your medical information online	20	29	58	55
P5. You believe it is fine to share your credit card details online	5	3	84	86
P6. You believe it is fine to share your (e.g. photo, video's) online.	20	16	50	64

Human	Public % Agree	Professional % Agree	Public % Disagree	Professional % Disagree
H1: Among your peers, you are among the first who try out new information technologies.	36	27	33	32
H2: You like to experiment with new information technologies.	66	58	11	9
H3: Employees (and patients) are enthusiastic about the cloud computing technology adoption in healthcare services.	50	44	13	19
H4: Employees (and patients) are ready to accept the changes caused by the cloud computing technology adoption in healthcare services.	45	43	17	19

Compatible	Public % agree	Professional % Agree	Public % Disagree	Professional % Disagree
T30: Adopting cloud technology in healthcare is compatible with current healthcare services practices.	52	67	8	16
T31: Adopting cloud technology is compatible with hospital's core values and goals.	60	63	4	13
T32: Adopting cloud technology is compatible with current information infrastructure in the hospitals.	47	55	14	19

B.9 : Healthcare Professional

Organisational - Relative Advantage	Professional % Agree	Professional % Disagree
O1: Adopting cloud computing technology in healthcare services can improve the collaboration and communication between professionals involved in the patient treatment plan.	73	9
O2: Adopting cloud computing technology in healthcare services can reduce the operating costs.	59	10
O3: Cloud computing technology can provide more timely access to patient information.	73	7

Organisational -Top Management Support	Professional % Agree	Professional % Disagree
O4: Top managers are likely to support the adoption of cloud computing technology in healthcare services.	51	12
O5: Top managers are likely to provide sufficient resources in adopting cloud technology in healthcare services.	47	9
O6: Top manager are likely to understand the benefits of cloud technology in healthcare services.	54	8
O7: Top manager are likely to encourage the development of cloud computing technology healthcare services.	54	10

Organisational - Adequate resource	Professional % Agree	Professional % Disagree
O8: Hospitals have sufficient IT infrastructure to support the development of cloud computing technology in healthcare services.	39	18
O9: Hospitals have enough human resources to develop cloud computing technology in healthcare services.	38	25
O10: Hospitals have enough time to develop cloud-computing technology in healthcare services.	37	20
O11: Hospital have enough budget to develop cloud-computing technology in healthcare services.	34	25

Organisational -Benefit	Professional % Agree	Professional % Disagree
O12: Adopting cloud computing technology can improve hospital image and expertise.	68	6
O13: Adopting cloud computing technology can improve internal efficiency.	67	5
O14: Adopting cloud computing technology can improve healthcare service quality.	67	4
O15: Adopting cloud computing technology can improve the relationship between hospital and patient.	60	7
O16: Adopting cloud computing technology can provide 24x7 worldwide accessibility to medical records.	67	4
O17: Adopting cloud computing technology will reduce duplicate patient tests.	70	6
O18: Adopting cloud computing technology can reduce time needed for doctors to access the patient treatment plan.	73	4
O19: Adopting cloud computing technology can increase health research and collaboration between various healthcare providers.	73	3
O20: Adopting cloud computing technology can improve the reliability of IT resources to avoid server break down or data loss.	67	4

Environmental	Professional % Agree	Professional % Disagree
E1: Healthcare cloud computing development is a key priority for the government.	46	14
E2: The government should develop Electronic Medical Records using cloud computing.	61	4
E3: Training courses on how to use cloud computing technology in healthcare should be provided by the government.	74	5
E4: High quality of training programs will be provided by the Cloud provider.	61	2
E5: High quality of training programs will be provided by the Hospitals.	57	5
E6: High quality of ongoing technical support will be provided by the Cloud provider.	57	5

13 Appendix C: Generic Reference Risk Register Table

No	Risk Type	Risk Name/ Description	Impact	Likelihood	Risk Level	Risk Perception	Security Goal	Security countermeasure
1	Security	Safeguarding patient confidential information and compliance	Very High	Medium	High	Confidentiality	Confidentiality Integrity Accountability Auditability	<i>Technical:</i> Dr. must have the right authentication and authorisation based on his role on storing medical health records and safeguarding it with key security regulations.
		<i>Description</i> Risk of Doctor disclosure of patient confidential information to someone else from the diagnose process.	<p>Sources: Mapped from ENISA 2012 Management interface compromise (manipulation, availability of infrastructure)</p> <p>ISO27799:2008</p> <p>7.8.1.2 Access control policy</p> <p>The organization's policy on access control should be established on the basis of predefined roles with associated authorities which are consistent with, but limited to, the needs of that role.</p> <p>The access control policy, as a component of the information security policy framework described in 7.2.1 Information security policy document shall reflect professional, ethical, legal and subject-of-care-related requirements and should take account of the tasks performed by health professionals and the task's workflow.</p>					

		The importance of this risk to the healthcare context in Oman	Medium- within Oman hospital medical staff tend to reveal medical information to family member or a friend without recognising that this action considers a breach of security. Thus, there is a need for awareness of disclosing patient information.					
2	Security	Health records accessible <i>Description:</i> The risk of Doctor retrieves the results of another patient from health records.	Very High	Medium	High	Confidentiality	Confidentiality Privacy Availability	<i>Technical:</i> Dr needs authorization to access and retrieves the results of a patient within his team of care as well as supporting privacy guidelines
Sources: Mapped from ENISA 2012 Management interface compromise (manipulation, availability of infrastructure) ISO27799:2008 7.8.1.2 Access control policy The organization's policy on access control should be established on the basis of predefined roles with associated authorities that are consistent with, but limited to, the needs of that role.								
		The importance of this risk to the healthcare context in Oman	Low- Doctors are expected to check that this is the right patient before retrieves the results to avoid retrieving someone else results.					
3	Security	Identity theft	High	Low	Medium	Confidentiality Data Security	Confidentiality Authorization, Authentication and Auditing (AAA)	<i>Technical:</i> Apply Authorization, Authentication and Auditing (AAA) enforcing strong passwords creation. Only authorised parties granted access, ensuring that users do not gain access to other users' data.

		<i>Description</i> The fraudulent practice of using another person's name and personal information in order to obtain credit loans or other confidential details.	Mapped from EDoS ENISA 2012					
4	Security	Distributed Denial of service (DDoS) attacks. Ref: ENISA,2012	High	Medium	Medium	Availability Data security	Availability	<i>Technical:</i> Penetration testing to check and patch vulnerabilities.

		<p><i>Description</i> Preventing legitimate users from accessing their services in the cloud Leads to unavailability of resources and increases cloud usage bills</p>	<p>Source:</p> <p>7.7.5 Health information backup: In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information shall back up all personal health information and store it in a physically secure environment to ensure its future availability.</p> <p>7.7.6.2 Security of network services In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should carefully consider what impact the loss of network service availability will have upon clinical practice.</p> <p>7.10.1 Reporting information security events and weaknesses</p> <p>7.11 Information security aspects of business continuity management</p> <p>Disaster recovery, is increasingly recognised as a requirement for health organizations and the priority it is accorded continues to grow</p>					
		<p>The importance of this risk to the healthcare context in Oman</p>	<p>Medium- in Oman most of the traffic is controlled by Oman Gateway and OmanCert which is used in ITA-Cloud to filter all the attacks thus it can help to minimize the impact of DDoS</p>					
5	Security	<p>Economic Denial of Service (EDoS)</p> <p>Ref: ENISA,2012</p>	High	Low	Medium	Availability Data security	Availability	<p><i>Technical :</i></p> <p>Penetration testing to check and patch vulnerabilities reactive/on-demand in-cloud eDDoS mitigation service (scrubber service) for mitigating the application-layer and network-layer DDOS attacks with the help of an efficient client-puzzle approach.</p>

		Description: happen as a result of attacks, poor budget planning, or misconfigurations, the cost of a Cloud service can place pressure on the financial resources of a Cloud Customer to the point where the service is no longer affordable.					
		The importance of this risk to the healthcare context in Oman	Low – This is managed by ODP and ITA-Cloud				
6	Security	Insecure or ineffective deletion of data Ref: ENISA,2012	Very High	Medium	High	Integrity Privacy Integrity (accuracy)	<i>Legal:</i> Signing Service Level Agreement for critical data to destroy data as per user requirement.
		<i>Description</i> When a user request to delete his data from service provider in cloud, they cannot delete the entire disk as it shared by other users too.	Sources: 7.9.1 Security requirements of information systems Organizations processing personal health information should ensure that data from which personal identification can be derived is only retained where it is necessary to do so, and that deletion, anonymization and pseudonymization techniques are appropriately used to the full extent possible to minimize the risk of unintentional disclosures of personal information.				
		The importance of this risk to the healthcare context in Oman	Medium- X ministry need to specify in the service level agreement with ODP and ITA-Cloud the policy for deletion of data and how long for such action can take.				

7	Security	Federated authentication	High	High	High	Confidentiality	Confidentiality Authorization, Authentication and Auditing (AAA)	<i>Technical:</i> Only authorised parties granted access, ensuring that users do not gain access to other users' data. For example, single sign on, federated identity.	
		<i>Description</i> It delegates authentication to the organisations that use SaaS. As a user, the healthcare organisations must ensure that their cloud provider enforces security measures.	Mapped from ENISA for Data protection ENISA, 2012						
		The importance of this risk to the healthcare context in Oman	High- in Oman authority is given according to the role and responsibility. An organisation must ensure that their cloud provider enforces security measures						
8	Security	Loss of governance Ref: ENISA, 2012 .	Very high	Very high	Very High	Data security	Accountability	<i>Organisational:</i> - Clarify in detail in the Service Level Agreement (SLA) roles and responsibilities before cloud adoption. To avoid any miscommunication in future. -Use Service Level agreement to address the exact type of control needed over their data in cloud.	
		<i>Description</i> In using cloud infrastructures, the client necessarily give up							

		control to the Cloud Provider (CP) on a number of issues which may affect security. At the same time, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defences						
		The importance of this risk to the healthcare context in Oman	Low- according to Oman Data Park (ODP) and Information Technology Authority-Cloud (ITA-Cloud) each Ministry has to sign off service level agreement which indicates the type of control required over their data centre locally and how to act in case of emergency.					
9	Security	Data Lock-in Ref: ENISA 2012	Medium	High	High	Availability	Availability Confidentiality Integrity	<p><i>Technical:</i></p> <p>Mitigate IaaS lock-in risk by using middleware that is compatible with multiple clouds.</p> <p><i>Organisation:</i></p> <p>Organizations processing personal health information shall back up all personal health information and store it in a physically secure environment to ensure its future availability.</p> <p>To protect its confidentiality, personal health information should be backed up in an encrypted format.</p>

		<p><i>Description</i></p> <p>for SaaS/PaaS and system lock-in for IaaS in cloud computing it represents the situation where customers are dependent (i.e. locked-in) on a single cloud provider technology implementation and cannot easily move in the future to a different vendor without substantial costs, legal constraints, or technical incompatibilities</p>	<p>Source :</p> <p>ISO27799:2008</p> <p>7.7.5 Health information backup</p> <p>In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information shall back up all personal health information and store it in a physically secure environment to ensure its future availability.</p> <p>To protect its confidentiality, personal health information should be backed up in an encrypted format.</p> <p>7.7.10 Monitoring</p> <p>7.10.1 Reporting information security events and weaknesses</p>					
		<p>The importance of this risk to the healthcare context in Oman</p>	<p>Low- ODP and ITA- Cloud are responsible to manage those kind of risk as they are the only provider for cloud computing service in Oman</p>					
10	Security	<p>Intercepting data in transit Ref: ENISA,2012</p>	High	Medium	Medium	Confidentiality Data Security	Confidentiality Authentication Availability	<p><i>Technical:</i> Dr. and Nurse need to have the right authorisation and authentication when dealing with the referral form of the patient.</p> <p><i>Human Oriented:</i> Dr. and Nurse need to have security training awareness when processing the referral form.</p>
		<p><i>Description</i></p> <p>When the data move from one location to another</p>	<p>Sources:</p> <p>ISO27799:2016</p>					

		location through the internet or private network, there is risk data in transit or data at rest depends on security measures in place to secure the data. there is high possibility the transfer can be intercepted for instance between Cloud Customer and Cloud Provider	13.2.2 Agreements on information transfer As noted in 13.2.1, specific guidance on health information exchange policies can be found in ISO 22857. Though that International Standard explicitly references trans-border flow of personal health information (where borders in this context represent health jurisdictions, not necessarily national boundaries), much of its advice can be adapted, where necessary, to deal with exchange of data from one organization to another. ISO/IEC 27002:2013, 13.2.1 which is Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.					
		The importance of this risk to the healthcare context in Oman	Medium –currently it clouds computing is not used however, Man In the Middle (MIM) can control the data between hospital and cloud.					
11	Security	Data protection risks Ref: ENISA,2012	High	High	High	Data Security	Confidentiality Privacy Cryptography	<i>Human Oriented</i> patient should keep his record in locked bag with need pin code to access to avoid unauthorised access. <i>Technical:</i> Doctor should protect Patient medical information from unauthorized access. Organisational: based on security procedure within the GP to consult another specialist to confirm patient results in top confidential process to confirm Dr. suspect

		<p><i>Description</i> patient need to secure his hard copy report and CDs of performed results in secure place.</p> <p>Whereas in Germany hospital, there is a need for GDPR compliance as patient needs to give consent for accessing their records.</p>	<p>Sources:</p> <p>ISO27799:2008 7.12.2.2 Data protection and privacy of personal information</p> <p>In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should manage informational consent of subjects of care.</p> <p>Where possible, informational consent of subjects of care should be obtained before personal health information is e-mailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organization.</p>					
		<p>The importance of this risk to the healthcare context in Oman</p>	<p>Low- ODP and ITA-Cloud store the data centrally in Oman according to Royal Degree thus it reduces the complication of rules and regulation of saving sensitive data abroad.</p> <p>As for Germany cloud provider it has to follow GDPR rules and regulations</p>					
12	Security	<p>Malicious insider Ref: ENISA,2012</p>	Very high	Medium	High	<p>Confidentiality Data Security Availability</p>	<p>Confidentiality Privacy Accountability Authenticity & Trustworthines</p>	<p><i>Technical:</i> specify and implement the access control policy for each member in the organisation according to their roles and responsibilities.</p> <p><i>Human Oriented:</i> organisation must provide security training workshop for all members to enhance their awareness of possible threats.</p> <p><i>Organisational:</i> Management in each organisation has to notify all members of security policy implemented</p>
		<p>Description Represents members who have authorized access to a</p>	<p>Source: From ISO27799:2008</p>					

		user's data may misuse it to perform malicious attacks on the users' PHR data. Mxoli et al. (2014)	7.8.1.2 Access control policy					
			7.5.1 Prior to employment					
			7.5.2 during employment					
			7.5.3 termination or change of employment					
		The importance of this risk to the healthcare context in Oman	High - this risk is applicable in every organisation as staff members may misuse their work rule in finding unauthorised information.					
13	Security	Identity and Access Management	High	Low	Medium	Confidentiality	Confidentiality Authorization, Authentication and Auditing (AAA)	<i>Technical:</i> apply Authorization, Authentication and Auditing (AAA) enforcing strong passwords creation. Only authorised parties granted access, ensuring that users do not gain access to other users' data.
		<i>Description</i> Identity and access management can be used to ensure that users with legitimate identity can access data.	Sources: Mapped from Economic Denial of Service ENISA 2012, ISO27799:2008 (7.8.2.1)					User registration procedures shall ensure that the level of authentication required of claimed user identity is consistent with the level(s) of access that will become available to the user.
		The importance of this risk to the healthcare context in Oman	Low – This is managed by ODP and ITA-Cloud					

14	Security	Physical intrusion Mxoli et al. (2014)	Very High	Medium	High	Confidentiality	Confidentiality Privacy	<i>Technical:</i> Authorisation use; physical security and biometric locks in critical locations.
		<i>Description</i> Cloud storage facilities are at a risk of being accessed by intruders which may compromise PHR data stored there. Mxoli et al. (2014)	Mapped from Cloud provider malicious insider - abuse of high privilege roles, ENISA 2012 Source: Organisational to enforce physical entry controls to offices should be secured, room and facilities should be secured, protection against external and environmental threat ISO27799:2008 7.6.1.2					
		The importance of this risk to the healthcare context in Oman	Medium- ODP and ITA- Cloud are responsible to manage the cloud storage					
15	Security	Third party access Mxoli et al. (2014)	Very High	Very High	Very High	Confidentiality Availability	Confidentiality Audit	<i>Technical:</i> measures that must be applied and/complied with for service levels to be achieved in reduced services, the arrangements for compliance auditing of the third-parties, and the penalties that will apply should any of these not be honoured. Information exchange agreements that specify the minimum set of controls to be implemented must also be used.

	<p>Collaboration is needed between two institution to exchange sensitive data. A Cloud provider can provide access to both institutions to view their sensitive data in a secure mode in the cloud however, a Cloud provider may decide to outsource the storage of some of their users' data to external parties . This increases the fear of unauthorized access to the user's PHR data</p>	<p>Sources: Mapped from Loss of governance ENISA, 2012 p22</p> <p>ISO27799: 2008</p> <p>7.3.3.1 Identification of risks related to external parties</p> <p>Organisation should implement Risk assessment to weight the risk by third party access. Then security control to be implemented according to risk level and technology used.</p> <p>7.3.3.3 Addressing security in third-party agreements</p> <p>7.7.8.1 Health information exchange policies and procedures and exchange agreements.</p>
	<p>The importance of this risk to the healthcare context in Oman</p>	<p>Low- ODP and ITA-Cloud hosted the data standalone centrally in Oman. However, MoH will need to sign an agreement with Germany hospital to exchange medical data which will change the impact to Medium level.</p>

16	Security	Multi-tenancy Mxoli et al. (2014)	High	High	High	Data Security	Confidentiality Integrity Availability	<p><i>Technical:</i> development, test and operation facilities should be separated (physically or virtually).</p> <p>Compartmentalization should be enforced to ensure that consumers may not access other users' information due to multi-tenancy. Cloud service provider should use effective encryption methods to guarantee data isolation between client: also, data fragmentation can be used.</p>	
		<p><i>Description</i> Different users share memory, networking capabilities etc. in Cloud Computing. This puts users' data at risks of being accessed by malicious attackers posing as PHR owners .</p> <p>Mxoli et al. (2014)</p>	<p>Sources: Mapped from Isolation failure ENISA 2012 p29 ISO27799:2008 7.7.1.4 Separation of development, test and operational facilities To separate physical or virtual and make sure that consumers do not have access due to Multi-tenancy.</p>						
		<p>The importance of this risk to the healthcare context in Oman</p>	<p>Medium – ODP and ITA-Cloud hosted the data standalone and no multi-tenancy carried out.</p>						

17		Loss of encryption Keys Ref: ENISA,2012	High	Low	Medium	Confidentiality	Availability Integrity	<i>Technical:</i> There are various ways to restate keys. One alternative is through using PKI. This mechanism assures the activation of the key in a secured channel. Another alternative is via the usage of a mobile SIM card which enables a one-time password to be used in the activation process.
	Security	The loss or compromise of cryptographic keys used for encryption, authentication or digital signatures can lead to data loss, denial of services, or financial damages Ref: ENISA,2012	Sources: Mxoli et al. (2014); (Citrix, 2014). Use Wireshark network analysis to rebuild the traffic based on the gathered keys. These keys can be used to decrypt the concerned traffic					
		The importance of this risk to the healthcare context in Oman	Low as ODP and ITA-Cloud follow high security standards as ISO 20000 and ISO 27000 which provide sense of assurance and security. However, the level will be high in case it happens within ODP and ITA-Cloud.					

18	Security	Software intrusions Mxoli et al. (2014)	Medium	Medium	Medium	Data Security	Confidentiality Integrity Availability Authenticity & Trustworthiness	<i>Technical:</i> Organizations processing sensitive information shall implement appropriate prevention, detection and response controls to protect against malicious software and shall implement appropriate user awareness training.	
		Description A user's PHR may be attacked by malware which can compromise their sensitive information such as login details [23]. Mxoli et al. (2014)	Mapped from Licensing Issues, ENISA 2012 p47 Source: Organisational (procedure) and Human oriented (security awareness and training) ISO27799:2008 7.7.4.1 In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information shall implement appropriate prevention, detection and response controls to protect against malicious software and shall implement appropriate user awareness training.						
		The importance of this risk to the healthcare context in Oman	Medium- ODP and ITA- Cloud are responsible to manage the software as well as arrange for awareness and training workshop for data security for hospital staff.						
19	Security	Data Privacy and security	High	High	High	Data Security	Privacy Availability	<i>Human oriented:</i> Transactional process needs to be carried out by security experts to make sure that there is no illegal activity	

		<p><i>Description</i></p> <p>it encompasses issues related to confidentiality, integrity, and availability of data should be ensured not only in enterprise storage and cloud storage, but also between different cloud storage services (Shirazi et al., 2017).</p>	<p>Sources: Mapped from Data protection risk , ENISA 2012 p 45</p> <p>ISO27799:2008 7.12.2.2 Data protection and privacy of personal information</p> <p>In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should manage informational consent of subjects of care.</p> <p>Where possible, informational consent of subjects of care should be obtained before personal health information is e-mailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organization.</p>					
		<p>The importance of this risk to the healthcare context in Oman</p>	<p>High – it will be high in Oman because it is dealing with three objective of patient data which is confidentiality, integrity, and availability.</p>					
20	Security	<p>Social engineering attacks (impersonation)</p> <p>Ref: ENISA, 2012</p>	High	Medium	Medium	<p>Data Security</p> <p>Internet based services (indirect)</p> <p>Privacy</p>	<p>Privacy</p>	<p><i>Human Oriented:</i></p> <p>Security awareness training needs to be performed to ensure information security.</p>
		<p>Using people to get confidential information.</p> <p>Ref: ENISA, 2012</p>						

		The importance of this risk to the healthcare context in Oman	High- in Oman there is lack of awareness of security programs. There is a need for mitigation strategy to deal with those kinds of risks within cloud environment. thus, ODP and ITA-cloud need to provide security training workshop for hospital staff.					
21	Security	Third-party storage servers are a target for hackers that may lead to a breach of the PHI (Li et al., 2013).	High	Medium	Medium	Confidentiality	Confidentiality	<i>Technical:</i> Encrypt all medical records before outsourcing to the cloud (Li et al., 2013).
		The importance of this risk to the healthcare context in Oman	Low- not stored on third party as part of Service Level Agreement					
22	Security	Security and privacy of medical data	Very high	Medium	Medium	Confidentiality	Confidentiality	<i>Organisation:</i> There is a need to decide high level of protection in the service level agreement to avoid any medical data leakage

		<p>Description</p> <p>Security and privacy of medical data from any threats or attacks are one of the main reasons for many enterprises that do not intend to employ cloud services (Seddona and Currie, 2013).</p>					
		<p>The importance of this risk to the healthcare context in Oman</p>	Low- storing the data centrally minimize a lot of risks.				
23	Management	<p>Reduced staff productivity</p>	High	Medium	Medium	Professional Environmental (Technical Competence	<p>Gap</p> <p><i>Human Oriented:</i></p> <p>Ensure that experts are not dismissed and involve them in the migration project so that they get a sense of ownership. Provide training in cloud technology and enable staff to learn new skills.</p>
		<p>During the migration as changes to staff work and job uncertainty lead to low staff self-esteem and nervousness spreading in the organisation.</p>					

		The importance of this risk to the healthcare context in Oman	Medium- the move to cloud will be huge change to hospital infrastructure. Thus, it needs careful consideration about the time and training needed to use new system infrastructure. This risk has critical effect on the work productivity as it can reduce the daily achievement by not keeping track on the daily work plan.				
24	Management	Managing a system deployed on several clouds	Very high	Medium	Medium	Professional organisational Top Management support	<i>Organisational:</i> Procedure to make management aware of the extra effort that might be required. Indicator: using several cloud providers for a system, as cloud providers have different types of support mechanisms.
		<i>Description:</i> Managing a system deployed on several clouds can make extra management effort compared to deploying systems in-house to ensure data availability.					
		The importance of this risk to the healthcare context in Oman	Low- because Ministry of Health (MoH) use central institutional data centre which is managed by ODP and ITA-Cloud				

25	Management	Employee resist change	High	High	High	Gap	Gap	<p><i>Organisational:</i></p> <p>Government and senior management need to provide positive leadership and support for employees to accept cloud computing as a new service because it will encourage employees to embrace it as new way of increasing the quality of work</p>	
		Description: Employee resist change to use new information technology (Lian et al., 2014; Alkhater et al., 2017)..							
		The importance of this risk to the healthcare context in Oman	High – this risk has a significant rule in the success or failure of a project. Healthcare organisation need to arrange for awareness training workshop for employees to accept the change and gain benefits of the new service from information technology						
26	Management	Lack of IS IS staff skills	Medium	Medium	Medium	Gap	Gap	<p><i>Human Oriented:</i></p> <p>Arrange for training courses to provide enough knowledge of skills needed to deal with cloud computing</p>	

		Description : IS staff need to have sufficient knowledge, awareness and the required skills to adopt cloud computing (Lian et al., 2014).						
		The importance of this risk to the healthcare context in Oman	Medium- Ministry of Health (MoH) in Oman has launched cloud infrastructure to host ministry website. MoH need to provide training course for IS staff to deal with cloud computing. The medical data is owned by hospital, used by doctor and custodian by other hospital. Thus the training courses are need for data owner, custodian and user.					
27	Management	Maintain privacy for genomic data	Medium	Medium	Medium	Gap	Gap	<i>Technology:</i> Provide Single Sing On to registered users.
		Description Maintain privacy for genomic data especially with the blending of genomics with Internet technologies which shared among the network (Chow-White et al., 2015).						
		The importance of this risk to the healthcare context in Oman	Low- It is critical to assure the privacy of patient data among shared network however genomic data is not dealt with in Oman currently.					

28	Management	IS infrastructure	High	High	High	Gap	Gap	<p><i>Organisational:</i></p> <p>Organisation need to operate the versatility across different environments; scaling to accommodate large data centres; automating to create self-managed environments; and integration of non-cloud products into the cloud architecture</p> <p>(Joseph and Brown, 2017)</p>	
		Description Ensure IS infrastructure deliver the right quality of service.							
		The importance of this risk to the healthcare context in Oman	<p>Low - In Oman there is Oman Data Park (ODP) and Information Technology Authority (ITA) who provide IS infrastructure, and smoothing the transfer process. ODT and ITA act like data centre. According to the royal degree it is not allowed to hold cloud outside Oman. Thus, risks of storing data abroad are low. In addition, ODT and ITA are compliance with the data centre standard and properly accredited with ISO 20000 for IT service Management, ISO 27001 for information Security Management System</p>						
29	Management	Technology readiness	Medium	Medium	Medium	Gap	Gap	<p><i>Organisational:</i></p> <p>Organisation need to check their resources in terms of IT infrastructure and human whether they can be used to implement e-Gov cloud.</p>	

		<i>Description</i> Technology readiness, existence of the IT infrastructure and human resources (Alkhater et al., 2017)					
		The importance of this risk to the healthcare context in Oman	Medium- this is risk relevant to Oman because we have the IT infrastructure However, human readiness is an issue as there is a lack of local expertise				
30	Management	Lack of ICT skills	Medium	Medium	Medium	Professional Environmental (Government policy) and Technical competence Human domain indirect	<i>Human-oriented:</i> set up motivational short courses to motivate and educate staff about the benefits of using the new technology as well as training sessions to familiarise themselves with the new ICT.
		<i>Description</i> Health professionals do not always have the necessary ICT skills to use eHealth solutions or leverage the benefits of cloud computing solutions.					

		The importance of this risk to the healthcare context in Oman	High – currently in Oman we are operating the available vendors from abroad by acting like help desk. We have shortage in-house skills because we depend on third party to fix or maintain an equipment. Thus, there is a need to have in-house skills.					
31	Management	High bandwidth and internet speed	High	High	High	Gap	Gap	<i>Organisational:</i> Organisations need to have a robust technical infrastructure and the necessary technical skills to adopt new technical services.
		Description High bandwidth and internet speed play an important role in an organisation's decision to employ cloud services.						
		The importance of this risk to the healthcare context in Oman	High- this is relevant to Oman as hospitals in the capital already have fibre -optic installed whereas as hospitals in the village suffer from low connection speed. Thus, there is a need to enhance internet connection with suitable bandwidth to be able to accept the new technical service.					
32	Technical	IS complexity and compatibility will affect IT adoption (Lin et al., 2012 and Liu, 2011).	High	High	High	Gap	Gap	<i>Organisational:</i> Organisation need to check the alignments of IT application systems to the cloud to check system compatibility in cloud. Having cloud computing compatibility with existing systems or applications in the hospital will help make the adoption of cloud computing technology feasible (Lian et al., 2014),(Lin et al., 2012 and Liu, 2011).

		<p>Description : IS complexity and compatibility will affect IT adoption (Lin et al., 2012 and Liu, 2011).</p> <p>For instance, migrate medical information system such as (PACS), (HIS) and (RIS) (Lian et al., 2014).</p>						
		<p>The importance of this risk to the healthcare context in Oman</p>	<p>High – because Oman depend on some abroad venders there is risk of complexity between two venders. In addition, compatibility issue will raise as two different vendor’s system might not be compatibility to each other. In addition, Oman has shortage of in-house expertise who are needed to deal with medical information system such as PACS, HIS and RIS.</p>					
33	Technical	<p>Losing control of a system’s infrastructure</p>	Medium	Medium	Medium	Gap	Gap	<p><i>Organisational:</i></p> <p>Before the adoption process, administrator can identify the system support in the service level agreement.</p>
		<p><i>Description</i></p>						
		<p>The importance of this risk to the healthcare context in Oman</p>	<p>Low- it depends on the package X ministry will choose is it like a service or infrastructure as there are different plan suggested to each customer according to their need. Those services are provided in Oman through Oman data Park (ODP) and Information Technology Authority (ITA). thus it depends on the requirement and facilities that MoH need.</p>					

34	Technical	Costs of the new IT investment play a significant role (Lian et al., 2014).	Low	Low	Low	Gap	Gap	<p><i>Organisational:</i></p> <p>Cloud Provider need to calculate the operation costs as adopting cloud computing requires different types of investment in such areas as hardware, software and system integration. The cost can be enormous due to the variable nature of the expenses (Lian et al., 2014).</p>
		<i>Description</i>						
		<p>The importance of this risk to the healthcare context in Oman</p> <p>Not relevant to MoH because its main concern will be on uploading and accessing the medical data whereas Cloud Provider (ODP and ITA) are responsible of calculating the costs.</p>						
35	Technical	Interoperability Issues	High	High	High	Gap	Gap	<p><i>Technology:</i></p> <p>Use cloud middleware to ease interoperability issues.</p> <p>Because of the limits of interoperability and security, no single vendor can provide a comprehensive, dominant solution serving both hospitals and smaller outpatient clinics (Jin and Chen, 2015).</p>

		<p><i>Description</i> Interoperation of healthcare systems such as maintaining HL7 in cloud-based environment (Jin and Chen, 2015; Lubamba and Bagula, 2017; Medical White Paper, 2018).</p>						
		<p>The importance of this risk to the healthcare context in Oman</p>	<p>High – Healthcare in Oman currently uses ICD system to record patient diagnoses and sends ICD message using the local cloud provider; on the other hand, global hospitals use HL7 to communicate with other healthcare provider. Thus there is risk of interoperability issues between Oman healthcare and international healthcare provider which can affect the availability of records</p>					
36	Technical	<p>Risks of new technologies such as IoT and mobile combined with cloud (Lubamba and Bagula, 2017).</p>	Low	Low	Low	Gap	Gap	<p><i>Technical:</i></p> <p>Infrastructure to support the impeded system for IoT.</p> <p><i>Organisational:</i></p> <p>Those risks need to be added to risk register.</p>
		<p><i>Description</i></p>						

		The importance of this risk to the healthcare context in Oman	Low- not relevant currently because IoT not implement yet. However, there is a need for Oman to revise the risk management approach once they adopt IoT					
37	Technical	Temporary outages: Mxoli et al. (2014)	High	Low	Medium	Availability	Availability Integrity	<i>Technical:</i> multiple cloud providers monitor applications from outside the cloud. Replicating the system across multiple clouds has associated costs and technical challenges.
		<i>Description</i> Cloud services can and do experience temporary outages which last for hours .it can causes major service interruption resulting in extensive outages and unavailability of services or loss of data.	Mapped from Resource exhaustion (under or over provisioning) ENISA, 2012 p27					
		The importance of this risk to the healthcare context in Oman	Medium- Ministry of Health (MoH) use Uninterrupted Power Supply (UPS) generators to ensure the service continuity.					
38	Technical	Data Loss and Leakage	High	High	High	Availability Integrity Data security	Availability Integrity	<i>Technical:</i> use Encryption key to encrypt the data before it is stored in the cloud
		<i>Description</i> Data Loss and Leakage could happen due to	Mapped from Isolation failure From ENISA 2012					

		numerous reasons, such as an operational failure, unreliable data storage, and inconsistent usage of encryption keys.						
		The importance of this risk to the healthcare context in Oman	Low- for infrastructure this is the responsibility of ODP and ITA-cloud. As for clinicians within hospital there is a need for awareness and training about safe storage of sensitive data of patient.					
39	Technical	Loss of backup Ref: ENISA,2012	low	Low	Medium	Availability Integrity Data security	Availability Privacy	<i>Technical:</i> use multiple cloud providers, monitor applications from outside the cloud. Replicating the system across multiple clouds has associated costs and technical challenges
		<i>Description</i> The backups a Cloud Provider makes of it's customers' data can get lost, damaged, or the physical media on which the backup is stored can get stolen.						
		The importance of this risk to the healthcare context in Oman	Not relevant to Oman because the data are stored remotely centrally in Oman through O DP and ITA-Cloud.					

40	Technical	Resource exhaustion (under or over provisioning) Ref: ENISA, 2012	Medium	Medium	Medium	Organisational (Adequate resources)	Availability	<i>Organisational:</i> policy agreement to set up Resource Limit for each user by Cloud Provider or consider another cloud provider.	
		Description: Cloud provider might not be able to meet the increased demand currently or in future in certain resource or to maintain given service level							
		The importance of this risk to the healthcare context in Oman	Low- this is the responsibility of ODP and ITA-cloud						
41	Technical	Network breaks Ref: ENISA,2012	Medium	Medium	Medium	Availability Data Security ISO 20,000 Development of IT infrastructure can be one of the risks need to be address in future research	Availability	<i>Technical</i> Use multiple cloud provider in a different location to ensure data protection and minimise the loss. This will require additional costs.	

		<p><i>Description</i> Network Breaks which indicates the loss of Internet connectivity due to failures at the Cloud Customer's site or the Internet service provider, temporarily reduced network bandwidth on the path between Cloud Customer (CC) and Cloud Provider (CP), disruptions in the global Internet routing infrastructure leading to the loss of the network path between CC and CP, and failures of the CP's Internet connectivity</p>						
		<p>The importance of this risk to the healthcare context in Oman</p>	<p>This depends on the communication speed which is provided by the telecommunication companies as hospitals in capital might have fibre optic, however, rural hospital still using dial-up 56kps which does not work with cloud. Therefore, for those hospital who have fibre optic can use cloud computing service and state in the service level agreement the condition of network break.</p>					
42	Technical	Modifying network traffic	High	Low	low	Availability	Availability	<p><i>Technical :</i> Use multiple cloud provider.</p>

		<p><i>Description</i> If the network traffic is manipulated between user and cloud provider, this would result in loss of credibility.</p>	<p><i>Comments:</i> ISO 20,000 for the development of IT infrastructure could be one of the risks that needs to be addressed in future research.</p>					
		<p>The importance of this risk to the healthcare context in Oman</p>	<p>Low- as in Oman ODP and ITA-Cloud manage the network traffic. X Ministry can specify in the service level agreement the case of network traffic and what need to be done in case this incident happen.</p>					
43	Legal	<p>Risk from changes of jurisdiction Ref: ENISA,2012</p>	High	High	High	Out of scope	Legal	<p><i>Legal:</i> cloud customers need to be fully aware and understand the rules regarding where their data is held (Berry and Reisman, 2012).</p>

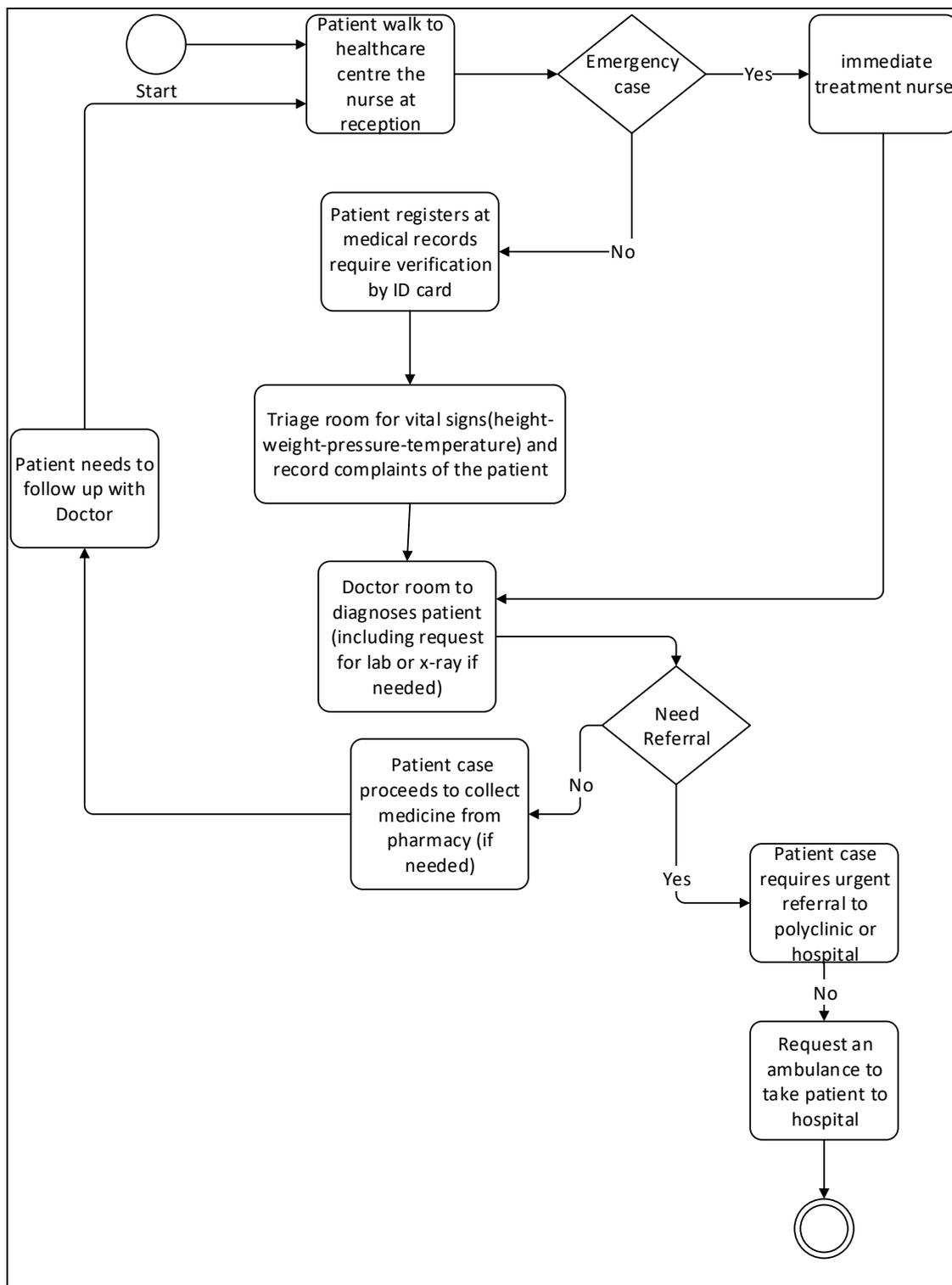
		<p><i>Description</i> When the data stored in different country than Cloud Customer's security of the information will be affected by various security risks.</p> <p>Because the Legal and regulatory framework of where data is held tend to change according to rules and regulation within the custodians country (Berry & Reisman, 2012).</p>						
		The importance of this risk to the healthcare context in Oman	Low- in Oman Cloud provider (ODP and ITA) hold all the data centrally according to Royal Degree.					
44	Legal	IT outsourcing	High	High	High	Gap	Gap	<p><i>Organisational:</i></p> <p>Provide high level of security with encryption to avoid any leakage during the transferring process</p>
		Description: IT outsourcing is significant as transferring health data among various legal and regulatory jurisdictions is						

		absolutely critical and requires a deep understanding of cloud outsourcing contracts (Iyer & Henderson, 2012). regulation and compliance need to be considered (Seddona and Currie, 2013).						
		The importance of this risk to the healthcare context in Oman	Low – in Oman is low because it stores data centrally.					
45	Legal	Address issues related to forensic and investigation shortcomings in cloud as well as lack of legal, judicial requirements and laws (Shirazi et al., 2017).	Medium	Medium	Medium	Gap	Gap	<i>Legal:</i> Organisation needs to consider from a different angle when operating in cloud environments, especially in the healthcare domain. Rules and regulation need to be expanded to provide more comprehensive impact and expose data to higher level of risk in cloud environment (Shirazi et al., 2017)..
		The importance of this risk to the healthcare context in Oman	Not relevant in Oman currently. In case they moved to store data aboard then there is a gap the legal judicial laws which need to be updated according to the case adopted.					
46	Others	Natural disasters Ref: ENISA,2012	High	Very low	Medium	Availability	Availability	Organisational Governance Strategy

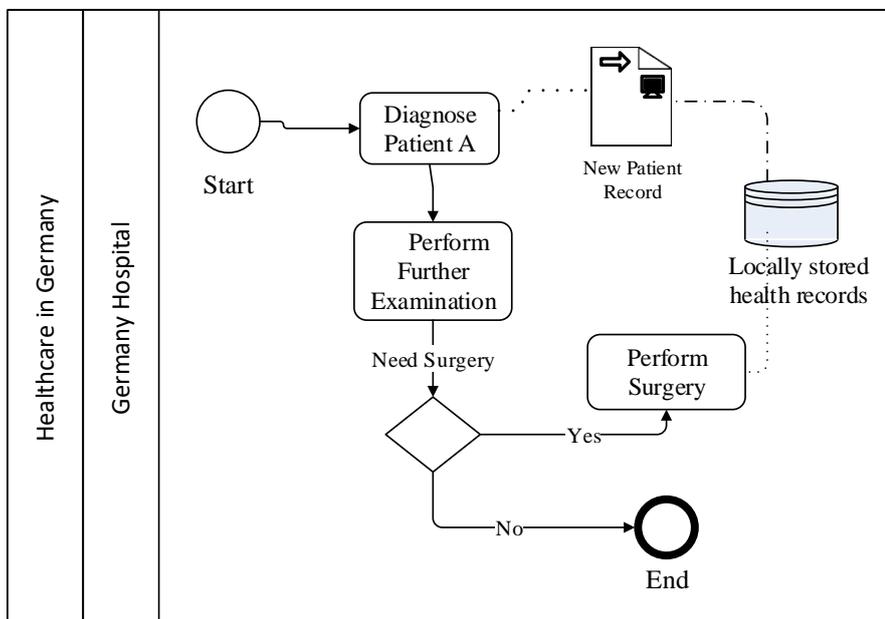
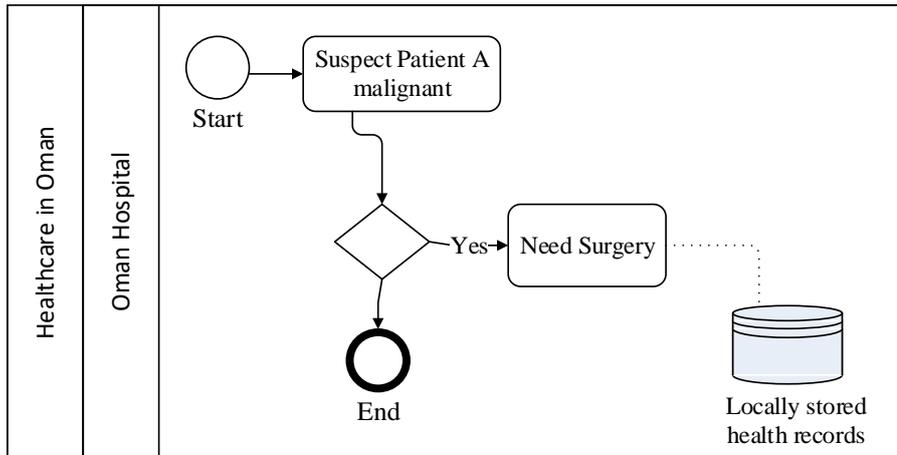
	<p><i>Description:</i> Natural disasters like flooding, earthquakes, tsunamis can affect the infrastructure of a CP. This way, a CC might be affected by natural disasters occurring far away from its own location.(ENISA,2012)</p>	<p>Note: ISO 22301 Business Continuity management approach can be considered as future work.</p>
	<p>The importance of this risk to the healthcare context in Oman</p>	<p>Medium- there is a need to maintain save backup abroad as Oman has several Cyclones from the Indian Ocean do occasionally make landfall in Oman in the summer months. For example: Cyclone Gonu (2007), Cyclone Phet (2010), Cyclonic Nilofar (2014), Cyclone Chapala (2015) and Cyclone Mekunu (2018), Thus the government of Oman need to maintain a backup abroad with the right rules and regulations.</p>

14 Appendix D: Hypothetical Scenario BPM and Risk Register Table

Appendix D 1: Generic Health Centre Workflow



Appendix D .2 First Modelling Attempt



Appendix D 2.1 Risk Register Table For First Modelling

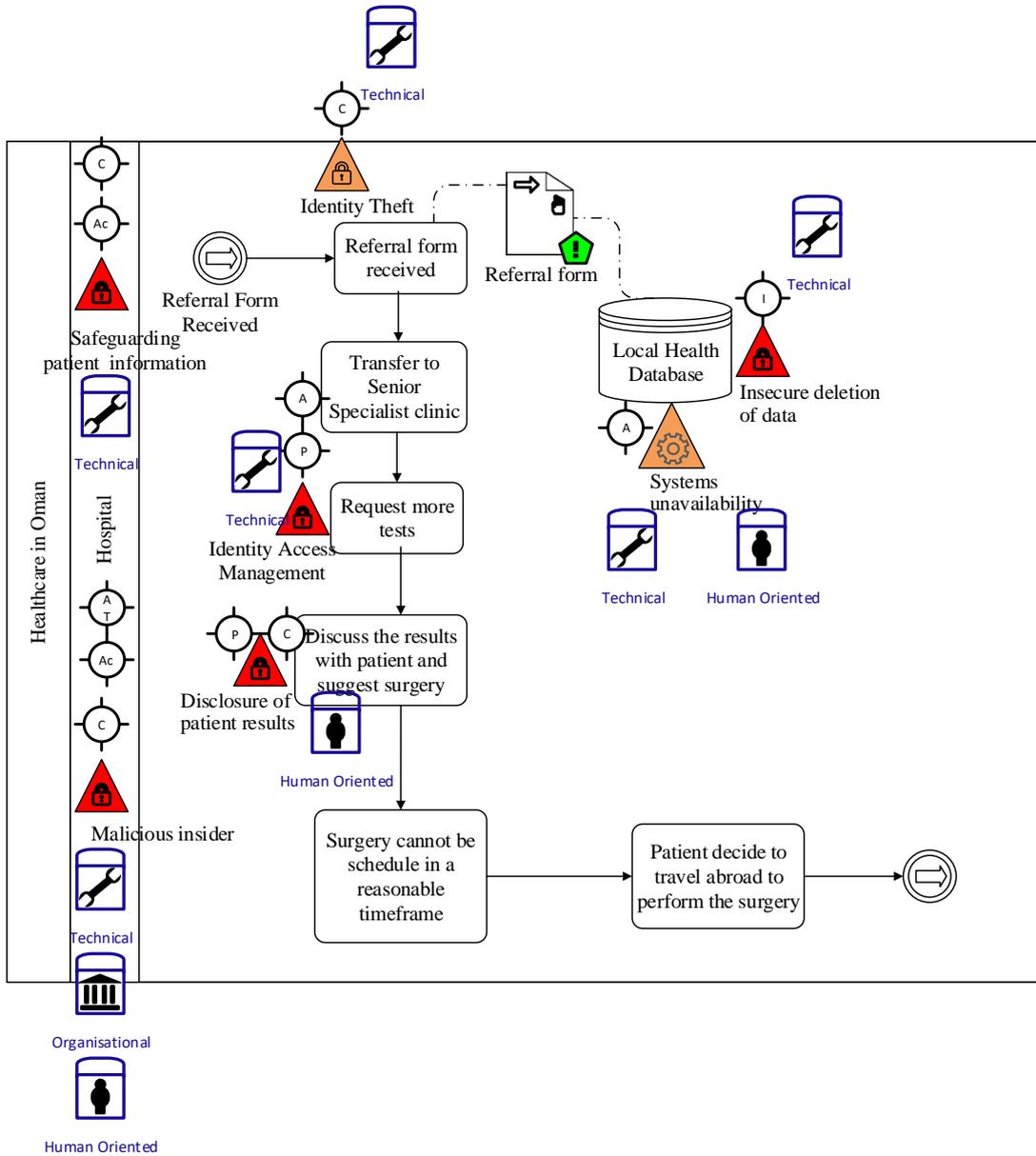
No	Risk Type	Risk Name/ Description	Impact	Likelihood	Risk Level	Security Goal	Countermeasure	Traceability
1	Security	Safeguarding Patient information A Primary investigation health record in Oman hospital <i>Description:</i> Safeguarding patient A health record in Oman hospital with key regulations	Very High	Medium	High	Confidentiality Accountability	Technical: implementing several layers of authentication such as user login, administration privilege based on their roles and need to access the data to secure health data records adequately	Oman hospital Activity: Suspect malignant head tumour
2	Security	Safeguarding Patient A Primary investigation health record in Germany hospital <i>Description:</i> Safeguarding patient A health record in Germany hospital with key regulations	Very High	Medium	High	Confidentiality Accountability	Technical: implementing several layers of authentication such as user login, administration privilege based on their roles and need to access the data to secure health data records adequately	Germany hospital Activity: Patient A diagnose

3	Security	<p>Identity and Access Management <i>Description:</i> Oman hospital implement security practices to access patient health record as well as supporting privacy guidelines</p>	Very High	Medium	High	Privacy Availability	<p>Technical: apply Authorization, Authentication and Auditing (AAA) enforcing strong passwords creation. Only authorised parties granted access, ensuring that users do not gain access to other users data.</p>	Oman hospital Activity: Need surgery
4	Security	<p>Identity and Access management <i>Description:</i> Germany hospital implement security practices to access patient health record as well as supporting privacy guidelines</p>	Very High	Medium	High	Privacy Availability	<p>Technical: apply Authorization, Authentication and Auditing (AAA) enforcing strong passwords creation. Only authorised parties granted access, ensuring that users do not gain access to other users data.</p>	Germany hospital Activity: further examination required

5	Security	<p>Malicious Insider: <i>Description</i> The risk of staff members in Oman hospital to misuse patient medical information</p>	Very High	Medium	High	Confidentiality Accountability Authenticity & Trustworthines s	<p>Technical Specify the access control policy for each member in the hospital according to their roles and responsibilities</p> <p>Human: hospital must provide security training workshop for all members to enhance their awareness of possible threats</p> <p>Organisation: hospital has to notify all members of security policy implemented in place.</p>	Oman hospital Process risk
---	----------	--	-----------	--------	------	--	--	-----------------------------------

6	Security	<p>Malicious Insider: <i>Description</i> The risk of staff members in Germany hospital to misuse patient medical information</p>	Very High	Medium	High	Confidentiality Accountability Authenticity & Trustworthines s	<p>Technical Specify the access control policy for each member in the hospital according to their roles and responsibilities</p> <p>Human: hospital must provide security training workshop for all members to enhance their awareness of possible threats</p> <p>Organisation: hospital has to notify all members of security policy implemented in place.</p>	Germany hospital Process risk
---	----------	---	-----------	--------	------	--	--	--------------------------------------

Appendix D.3 BPM for Hospital Process



Appendix D 3.1 Oman Hospital Risk Register Table

No	Risk Type	Risk Name/ Description	Impact	Likelihood	Risk Level	Security Goal	Countermeasure	Traceability
1	Security	<p>Safeguarding Patient information</p> <p><i>Description:</i> Safeguarding Nada's health record in Oman Hospital with key regulations</p>	Very High	Medium	High	Confidentiality Accountability	<p>Technical: implementing several layers of authentication such as user login, administration privilege based on their roles and need to access the data to secure health data records adequately</p>	Oman hospital Process risk

2	Security	<p>Malicious Insider: <i>Description</i> The risk of staff members in Oman hospital to misuse patient medical information</p>	Very High	Medium	High	Confidentiality Accountability Authenticity & Trustworthines s	<p>Technical Specify the access control policy for each member in the hospital according to their roles and responsibilities</p> <p>Human: hospital must provide security training workshop for all members to enhance their awareness of possible threats</p> <p>Organisation: hospital has to notify all members of security policy implemented in place.</p>	Oman hospital Process risk
3	Security	<p>Identity Theft <i>Description:</i> The fraudulent practice of using another person's name and personal information in order to obtain confidential details.</p>	High	Low	Medium	Confidentiality	<p>Technical Authentication based on smart card or certificate. physical identification. Activation required user finger print. the identity theft requires to obtain the card + the PIN number to access any system. End user must have the liability to ensure his PIN number is protected.</p>	Oman hospital Activity: Referral form received

4	Security	Identity and Access Management <i>Description:</i> Oman hospital implement security practices to access patient health record as well as supporting privacy guidelines	Very High	Medium	High	Privacy Availability	Technical: apply Authorization, Authentication and Auditing (AAA) enforcing strong passwords creation. Only authorised parties granted access, ensuring that users do not gain access to other users data.	Oman hospital Activity: request more tests
5	Security	Disclosure of patient results <i>Description</i> Doctor or nurse may disclosure patient results without the right permission or approval from the patient.	Medium	Medium	High	Confidentiality Privacy	Human Oriented Training course are need to ensure patient confidential information and how important it is to maintain his privacy all the time	Oman hospital Activity Discuss the results with patient and suggest surgery
6	Security	Insecure Deletion of Data <i>Description</i> When a patient request to delete his data from hospital database, they cannot delete the entire disk as it shared by other users too.	Very High	Medium	High	Integrity	Legal Signing Service Level Agreement for critical data to Destroy data as per user requirement.	Oman hospital

7	Technical	<p>System unavailability <i>Description:</i> there is a possibility of systems unavailability and this can be a major issue in an emergency situation where a doctor or nurse needs to access or updated patient information in the database.</p>	High	Low	Medium	Availability	<p>Technical include redundant CPUs, hot-swappable RAID drives with multiple access paths, controlling software for the high availability cluster, multiple LANs and WANs with all the redundant hardware and lines this implies, end user devices with multiple network adapters</p>	<p>Oman hospital Database</p>
---	-----------	---	------	-----	--------	--------------	---	--

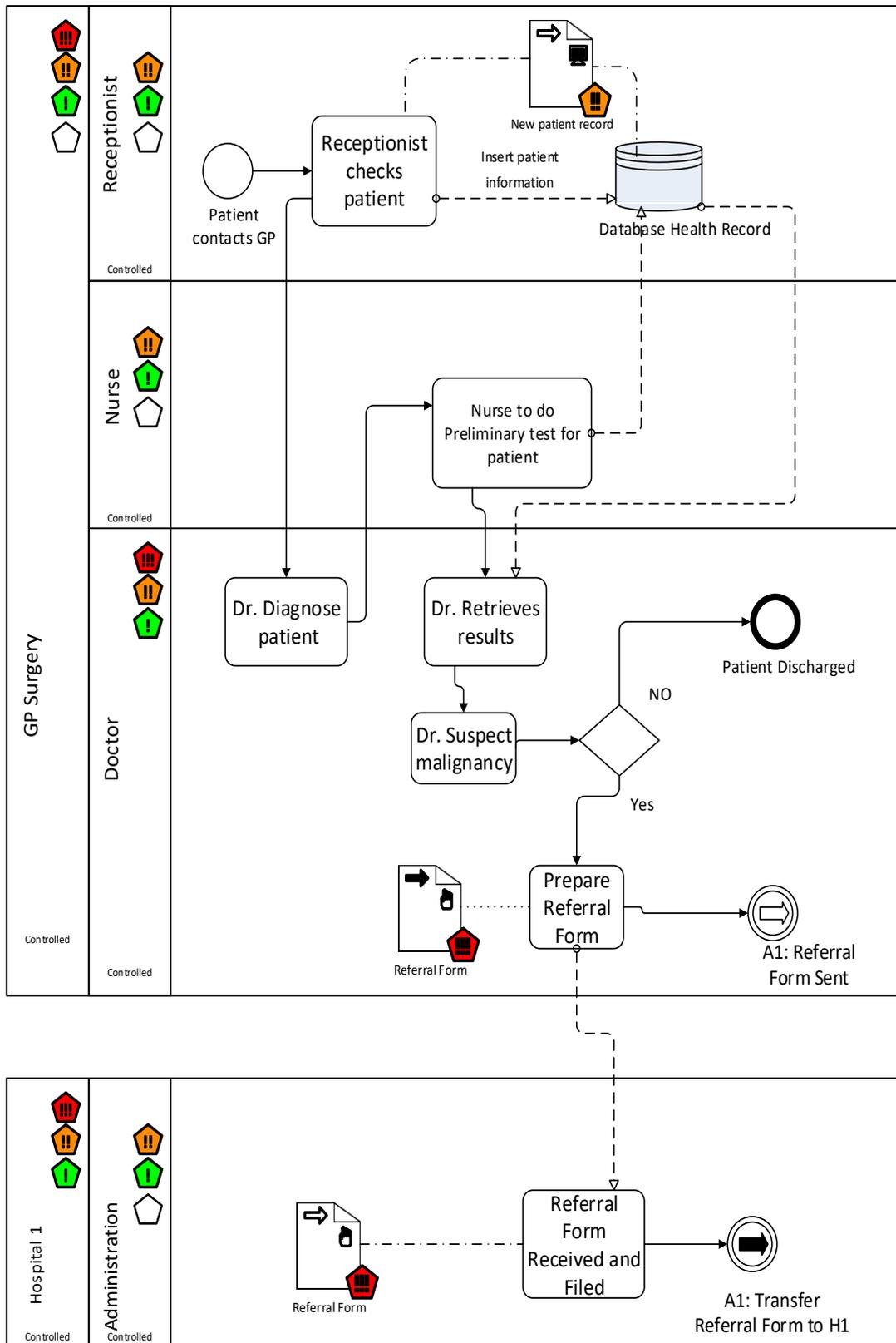
Appendix D 4.1 Patient Process Risk Register Table

No	Risk Type	Risk Name/ Description	Impact	Likelihood	Risk Level	Security Goal	Countermeasure	Traceability
1	Security	Third Party Access <i>Description:</i> there is a risk of third to access the hard copy of patient medical report without any permission.	Very High	Very High	Very High	Confidentiality Availability	<i>Human Oriented:</i> patient must secure the hardcopy report in safe bag or in safety box which needs a code to open to avoid any unauthorised access	Patient process
2	Security	Record could be Lost or Stolen <i>Description:</i> there is a risk of patient losing the hardcopy report	Medium	Medium	Medium	Availability	<i>Human Oriented:</i> patient should keep a scanned copy of the hard copy report in his email or in secure flash memory with code.	Patient process

3	Security	Data Protection: <i>Description:</i> patient need to secure his hard copy report and CDs of performed results in secure place.	High	High	High	Confidentiality	Human Oriented patient should keep his record in locked bag with need pin code to access to avoid unauthorised access.	Patient process
4	Security	Getting the Full Set of Report <i>Description:</i> there is a risk Printer ran out of paper and the printout is not the full set of the report.	Medium	Medium	Medium	Availability	Human Oriented Patient need to double check the page numbers of his report and ensure that he got the full set.	Patient process
5	Security	Imposter Another Patient Record <i>Description:</i> there is a risk of patient collecting another patient report by mistake.	Medium	Medium	Medium	Availability	Human Oriented Patient need to double check his personal details on the report before leaving the hospital to avoid any imposter with other patient details.	Patient process

15 Appendix E: Integrated Care Pathway

E.1 Full Set of BPM for Integrated Care Pathway



GP Surgery

Further Examination

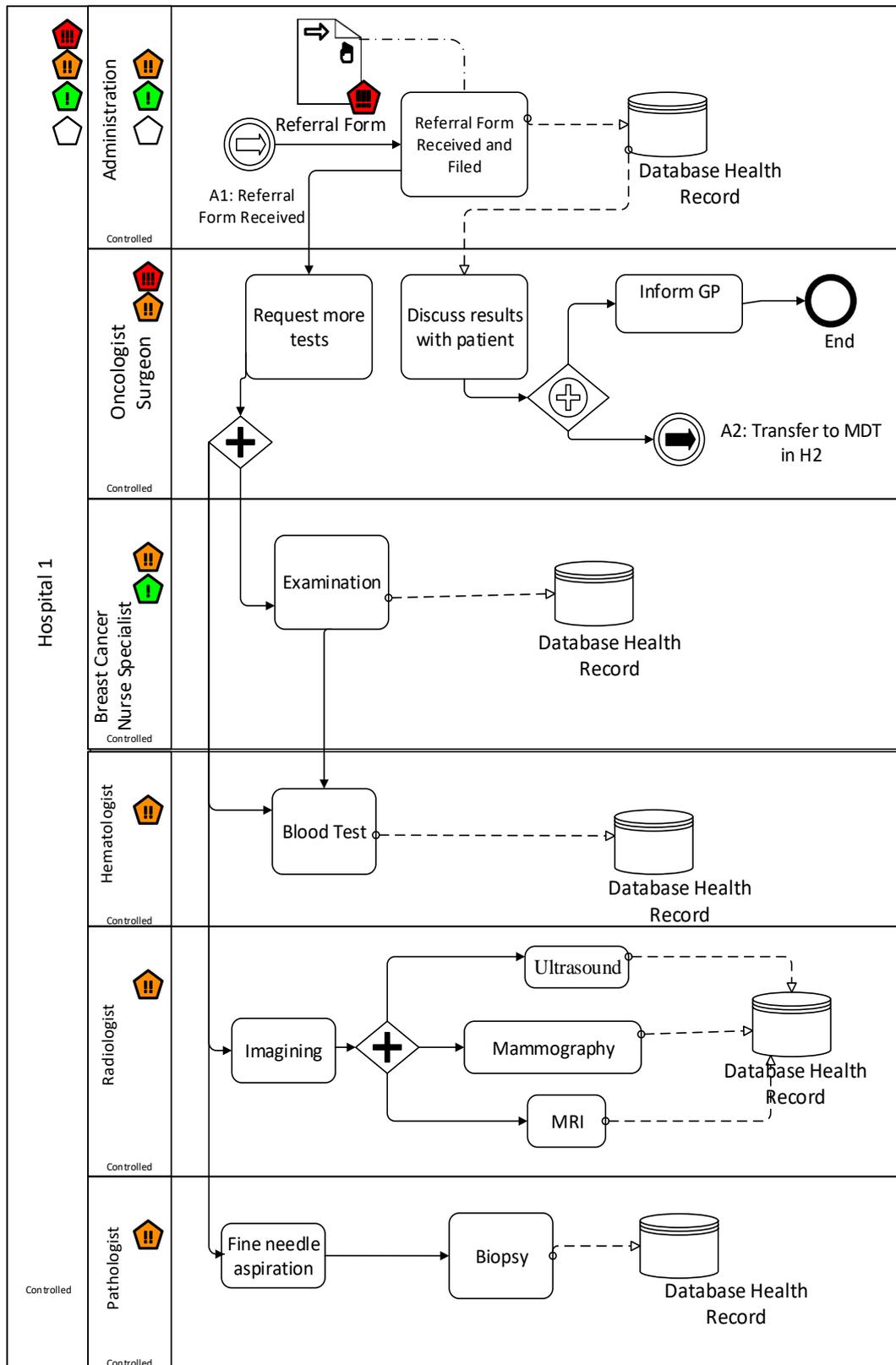


Figure Hospital 1 for Further Examination

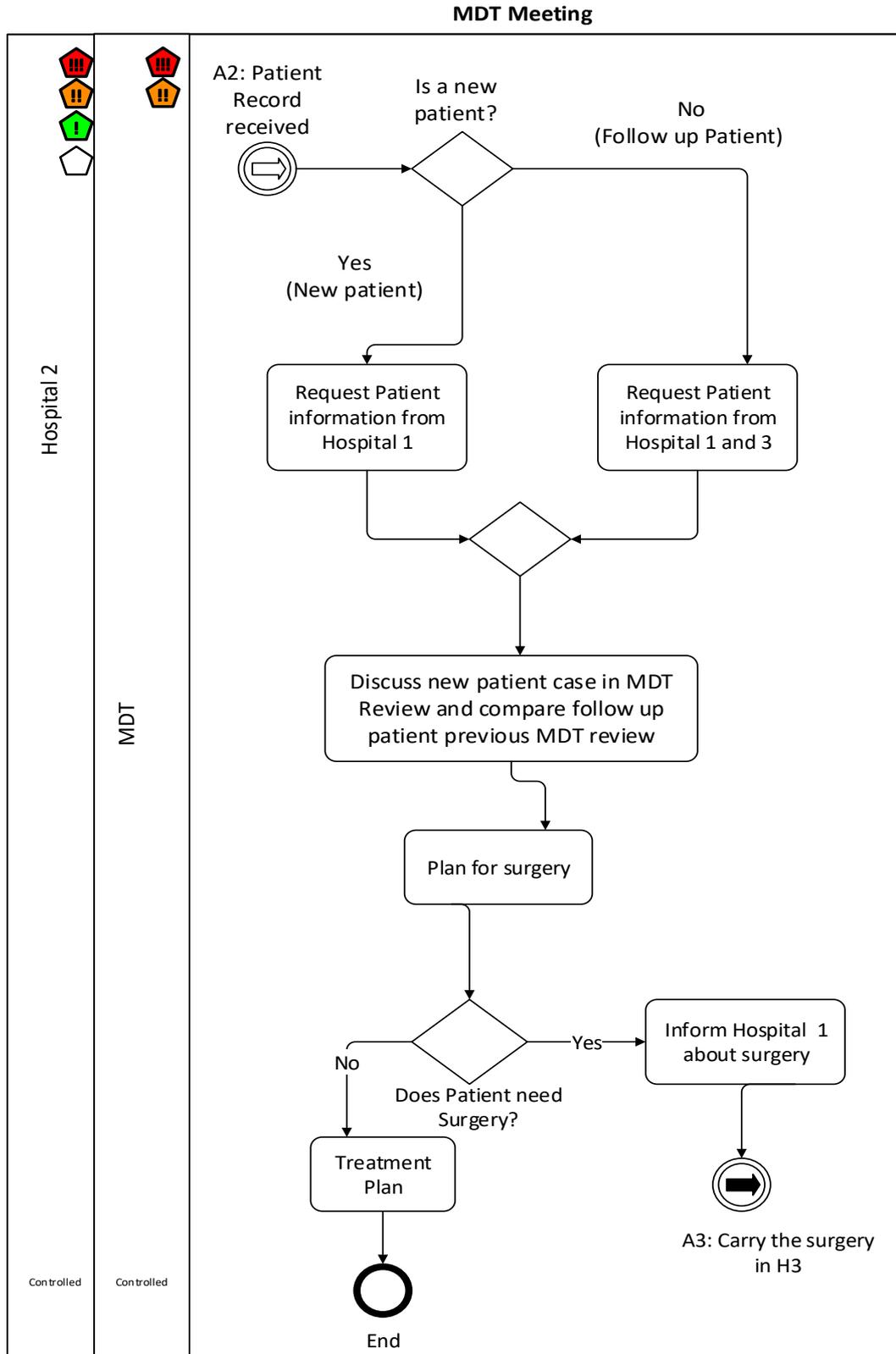


Figure: Hospital 2 for MDT Meeting

Perform Surgery

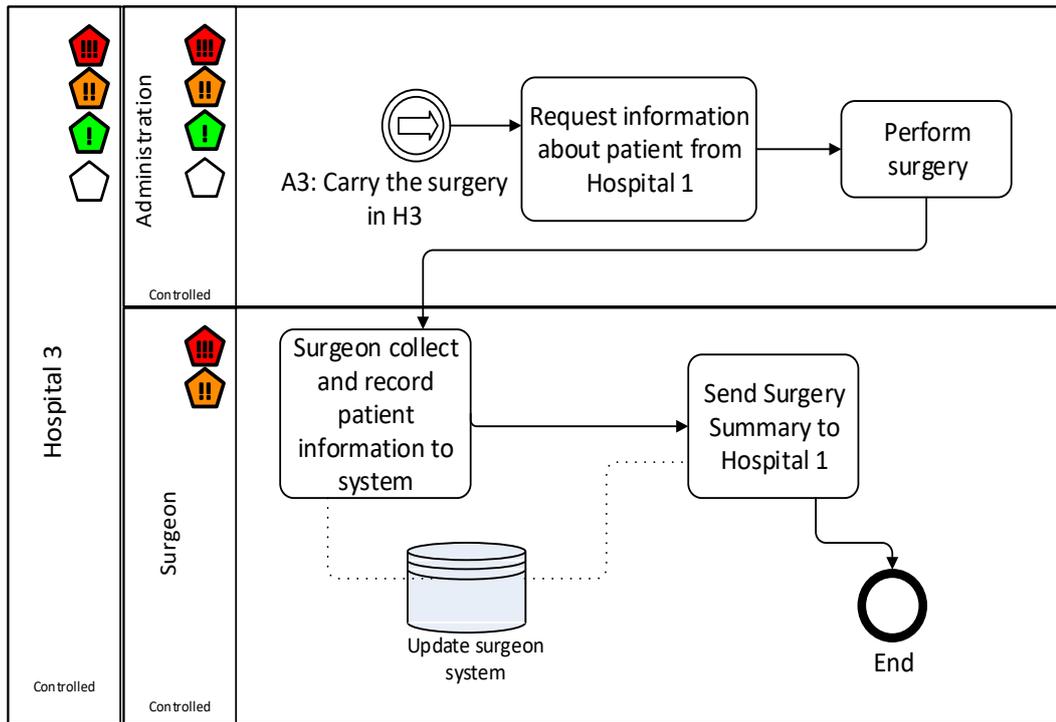
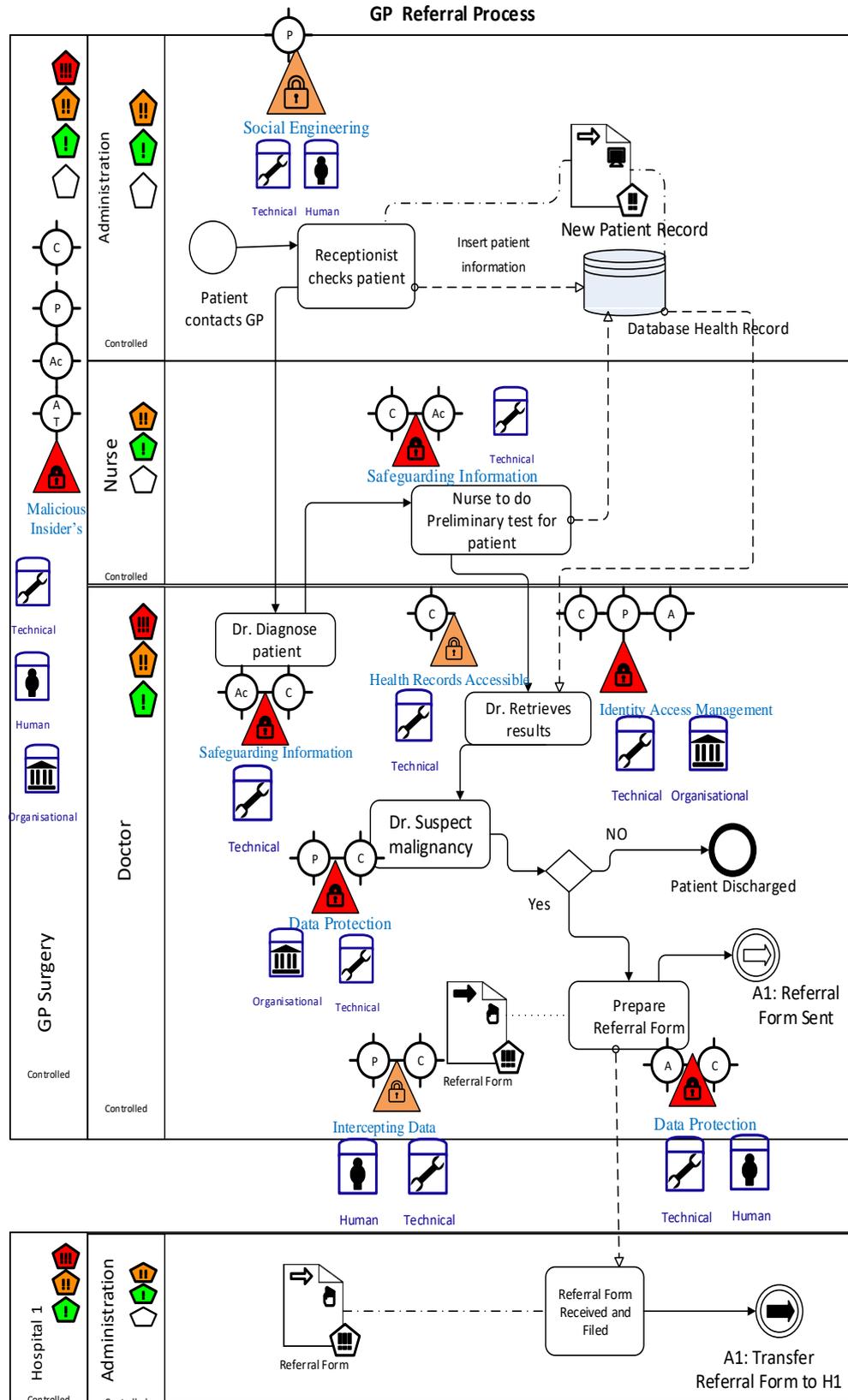


Figure : Hospital 3 to Perform Surgery

E.2 Patient Pathway in GP with Countermeasures



E.3 Risk Register for Patient pathway in GP Referral

No	Risk Type	Risk Name	Impact	Likelihood	Risk Level	Security Goals	Risk Countermeasure	Traceability	Date Identified/Modified
1	Security-15	<p>Malicious insider's</p> <p><i>Description</i> The risk of GP staff members to misuse patient medical information</p>	Very High	Medium	High	Confidentiality Privacy Accountability Authenticity & Trustworthiness	<p>Technical Specify the access control policy for each member in the GP Surgery according to their roles and responsibilities</p> <p>Human: GP must provide security training workshop for all members to enhance their awareness of possible threats</p> <p>Organisation: GP Surgery has to notify all members of security policy implemented in place.</p>	<p>Process: GP Referral</p> <p>Location: GP Surgery</p>	22 Feb 2017

Specific Activity Risk in GP Referral

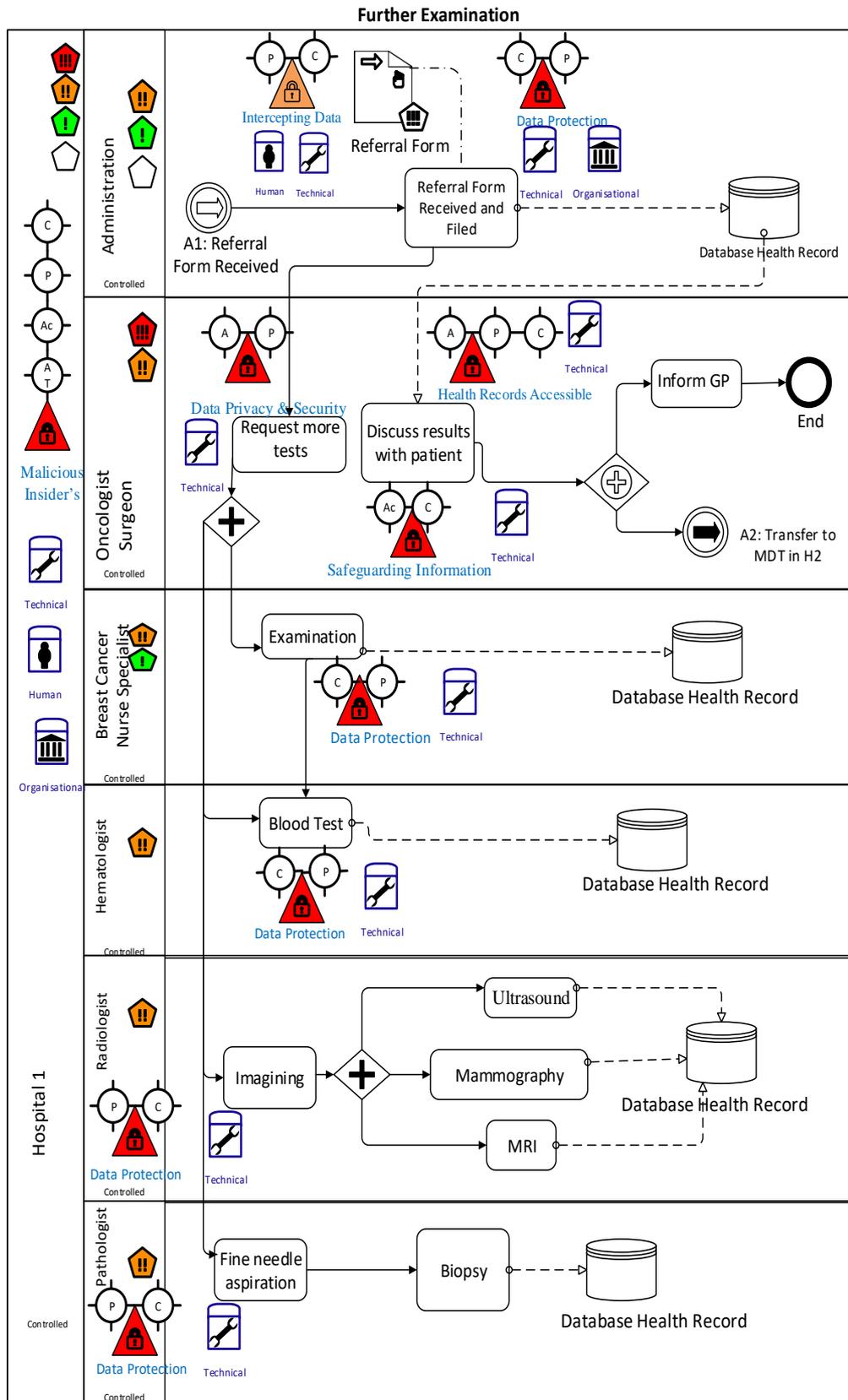
No	Risk Type	Risk Name	Impact	Likelihood	Risk Level	Security Goals	Risk Countermeasure	Traceability	Date Identified/ Modified
3	Security-24	<p>Social engineering attacks</p> <p><i>Description:</i> Risk of patient impersonate other patient details.</p>	High	Medium	Medium	Privacy	<p>Technical: Receptionist must check patient information by using fingerprint as validation process.</p> <p>Human: Security training for medical staff to ask security questions DoB, 1st line of patient address.</p>	<p>Process : GP Referral</p> <p>Location GP Surgery</p> <p>Activity: Receptionist checks patient</p>	22 Feb 2017

4	Security-1	<p>Safeguarding patient confidential information and compliance</p> <p><i>Description:</i> Risk of Doctor disclosure of patient confidential information to someone else from the diagnose process.</p>	Very High	Medium	High	Confidentiality Accountability	<p>Technical: Dr. must has the right authentication and authorisation based on his role on storing medical health records and safeguarding it with key security regulations.</p>	<p>Process : GP Referral</p> <p>Location GP Surgery</p> <p>Activity: Doctor Diagnose patient</p>	22 Feb 2017
5	Security-1	<p>Safeguarding patient confidential information and compliance</p> <p><i>Description:</i> The risk of Nurse disclosure patient results to someone else without the right approval during the preliminary tests conducted</p>	Very High	Medium	High	Confidentiality Accountability	<p>Technical: Nurse must has the right authentication and authorisation on storing patient results in the medical health records and safeguarding it with key security regulations</p>	<p>Process : GP Referral</p> <p>Location GP Surgery</p> <p>Activity: Nurse to do Preliminary test for patient</p>	22 Feb 2017

6	Security-2	Health records accessible <i>Description:</i> The risk of Doctor retrieves the results of another patient from health records.	Very High	Medium	High	Confidentiality Privacy Availability	Technical: Dr needs authorization to access and retrieves the results of a patient within his team of care as well as supporting privacy guidelines	Process : GP Referral Location GP Surgery Activity: Doctor Retrieves patient results	22 Feb 2017
7	Security-16	Identity Access Management <i>Description:</i> The risk of another Doctor using identity and access privilege of another Dr. to view patient results.	High	Low	Medium	Confidentiality	Technical: Dr. should use registration procedure to ensure the right authorization to access and retrieves patient results is consistent with his role and identity. Organisational: Dr. Should follow GP policy in retrieving patient results.	Process : GP Referral Location GP Surgery Activity: Doctor Retrieves patient results	22 Feb 2017

8	Security-14	<p>Data protection</p> <p><i>Description:</i> The risk of Doctor sharing suspect of malignancy based on results with another person without patient approval.</p>	High	High	High	Confidentiality Privacy	<p>Technical: Doctor should protect Patient medical information from unauthorized access.</p> <p>Organisational: based on security procedure within the GP to consult another specialist to confirm patient results in top confidential process to confirm Dr. suspect</p>	<p>Process : GP Referral</p> <p>Location GP Surgery</p> <p>Activity: Doctor Suspect of malignancy</p>	22 Feb 2017
9	Security-13	<p>Intercepting data in transit</p> <p><i>Description:</i> The risk of disclosure from Dr. or nurse when processing the referral form between different places, computers or sites</p>	High	Medium	Medium	Confidentiality Availability	<p>Technical: Dr. and Nurse need to have the right authorisation and authentication when dealing with the referral form of the patient.</p> <p>Human Oriented: Dr. and Nurse need to have security training awareness when processing the referral form.</p>	<p>Process: GP Referral</p> <p>Location GP Surgery</p> <p>Flow Dependence s: Referral Form transferred from GP Surgery to Hospital 1</p>	22 Feb 2017

E.4 Patient Pathway in Hospital 1 with Countermeasures



E.5 Risk Register for Patient Pathway in Hospital 1

No	Risk type	Risk Name	Impact	Likelihood	Risk Level	Security Goals	Risk Countermeasure	Traceability	Date Identified/ Modified
1	Security-15	<p>Malicious Insider's</p> <p><i>Description:</i> The risk of hospital 1 staff members to misuse their role on the patient medical records.</p>	Very high	Medium	High	Confidentiality Privacy Accountability Authenticity & Trustworthiness	<p>Technical: specify the access control policy for each member in Hospital 1 according to their roles and responsibilities</p> <p>Human: Hospital 1 must provide security training workshop for all members to enhance their awareness of possible threats</p> <p>Organisation: Hospital 2 has to notify all members of security policy implemented in place.</p>	<p>Process: Further Examination</p> <p>Location: Hospital 1</p>	22 Feb 2017

Patient pathway in Further Examination (Hospital 1) -Flow Dependencies Risk

No	Risk type	Risk Name	Impact	Likelihood	Risk Level	Security Goals	Risk Countermeasure	Traceability	Date Identified/ Modified
2	Security-13	<p>Intercepting Data in Transit</p> <p><i>Description:</i> The risk of disclosure from Dr. or Nurse when processing the referral form between different places, computers or sites</p>	High	Medium	Medium	Confidentiality Availability	<p>Technical: Dr. and Nurse need to have the right authorisation and authentication when dealing with the referral form of the patient.</p> <p>Human Oriented: Dr. and Nurse need to have security training awareness when processing the referral form.</p>	<p>Process: Further Examination</p> <p>Location: Hospital 1</p> <p>Activity : Referral Form</p>	22 Feb 2017

Activity risks in Further Examination (Hospital 1)

No	Risk Type	Risk Name	Impact	Likelihood	Risk Level	Security Goals	Risk Countermeasure	Traceability	Date Identified/ Modified
3	Security-14	Data Protection <i>Description:</i> The risk of Receptionist sharing Referral form details with another person without right approval.	High	High	High	Confidentiality Privacy	Technical: Receptionist should protect patient medical information from unauthorized access. Organisational: based on security procedure within the Hospital 1 to share or disclosure patient details with another person.	Process: Further Examination Location : Hospital 1 Activity : Referral Form Received and Filed	22 Feb 2017
4	Security-23	Data Privacy and security <i>Description:</i> The risk of sharing Oncologist Surgeon patient case with another person	High	High	High	Privacy Availability	Technical: Oncologist Surgeon needs to deal with patient medical data as highly sensitive according to Data Privacy and security regulations.	Process: Further Examination Location: Hospital 1 Activity : Request more tests	22 Feb 2017

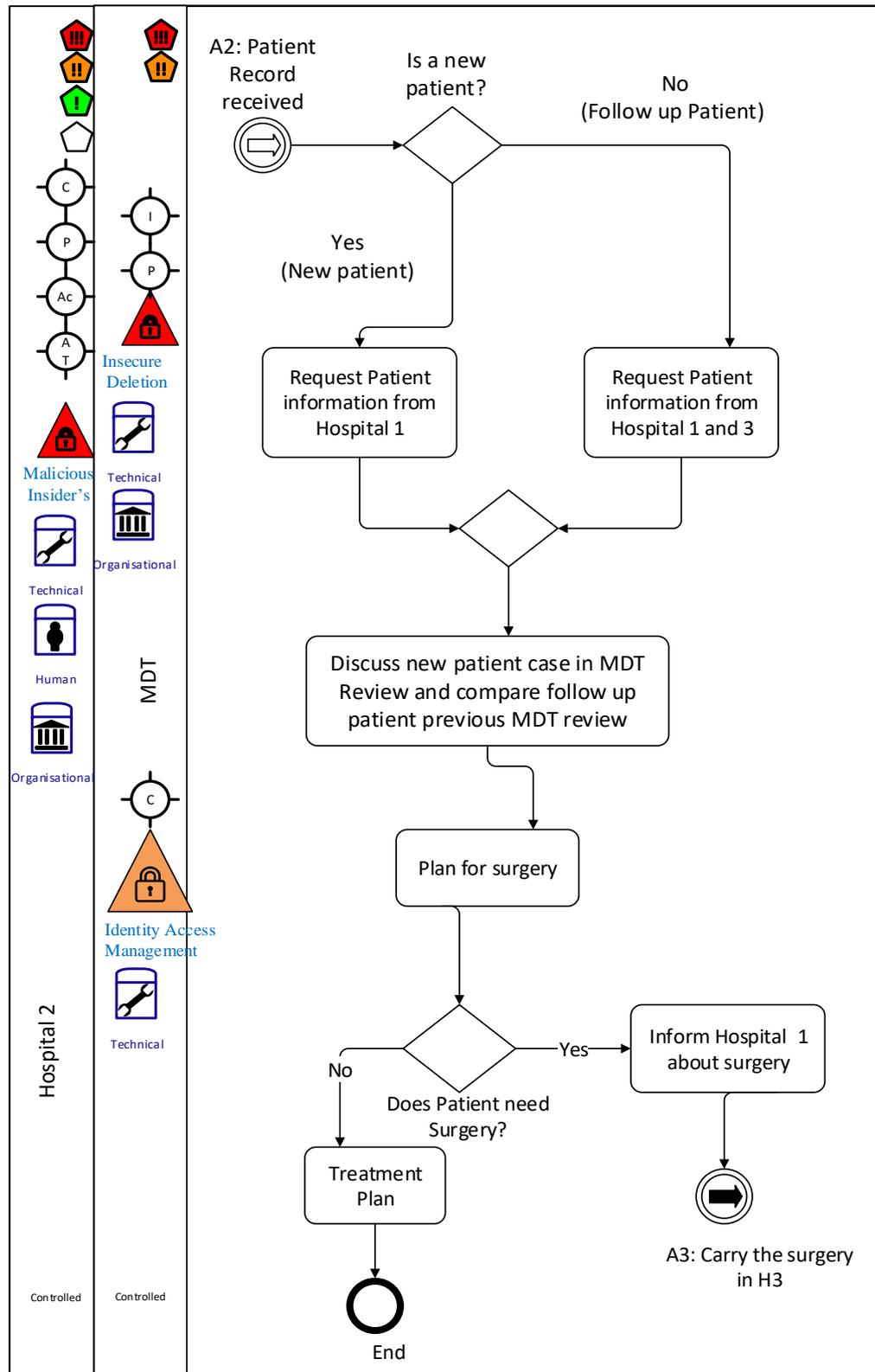
5	Security-1	<p>Safeguarding patient confidential information and compliance</p> <p><i>Description:</i> The risk from Oncologist Surgeon not safeguarding patient medical results and disclosure it with another person without the right approval.</p>	Very High	Medium	High	Confidentiality Accountability	<p>Technical: Oncologist Surgeon needs to safeguarding patient confidential information and compliance during the diagnose process. He must has the right authentication and authorisation on storing medical health records and safeguarding it with key security regulations.</p>	<p>Process: Further Examination</p> <p>Location: Hospital 1</p> <p>Activity : Discuss results with patient</p>	22 Feb 2017
---	------------	---	-----------	--------	------	-----------------------------------	--	--	-------------

6	Security-2	<p>Health Records Accessible</p> <p><i>Description:</i> The risk from Oncologist Surgeon retrieves the results of patient from health records is leaving it accessible to other members who is outside the care team of the patient.</p>	Very High	Medium	High	Confidentiality Privacy Availability	<p>Technical: Oncologist Surgeon needs authorization to access and retrieves the results of a patient within his team of care as well as supporting privacy guidelines</p>	<p>Process: Further Examination</p> <p>Location: Hospital 1</p> <p>Activity : Discuss results with patient</p>	22 Feb 2017
---	------------	---	-----------	--------	------	--	---	--	-------------

7	Security-14	Data Protection <i>Description:</i> The risk of Breast Cancer Nurse Specialist, Hematologis, Radiologist and Pathologist sharing patient results with someone else without the right approval.	High	High	High	Confidentiality Privacy	Technical: Breast Cancer Nurse Specialist, Hematologis, Radiologist and Pathologist should protect patient medical information from unauthorized access and not disclosure it to anyone.	Process: Further Examination Location: Hospital 1 Activity : Breast Cancer Nurse Specialist, Hematologis, Radiologist and Pathologist	22 Feb 2017
---	-------------	--	------	------	------	----------------------------	--	--	-------------

E.6 Patient Pathway in Hospital 2 with Countermeasures

MDT Meeting



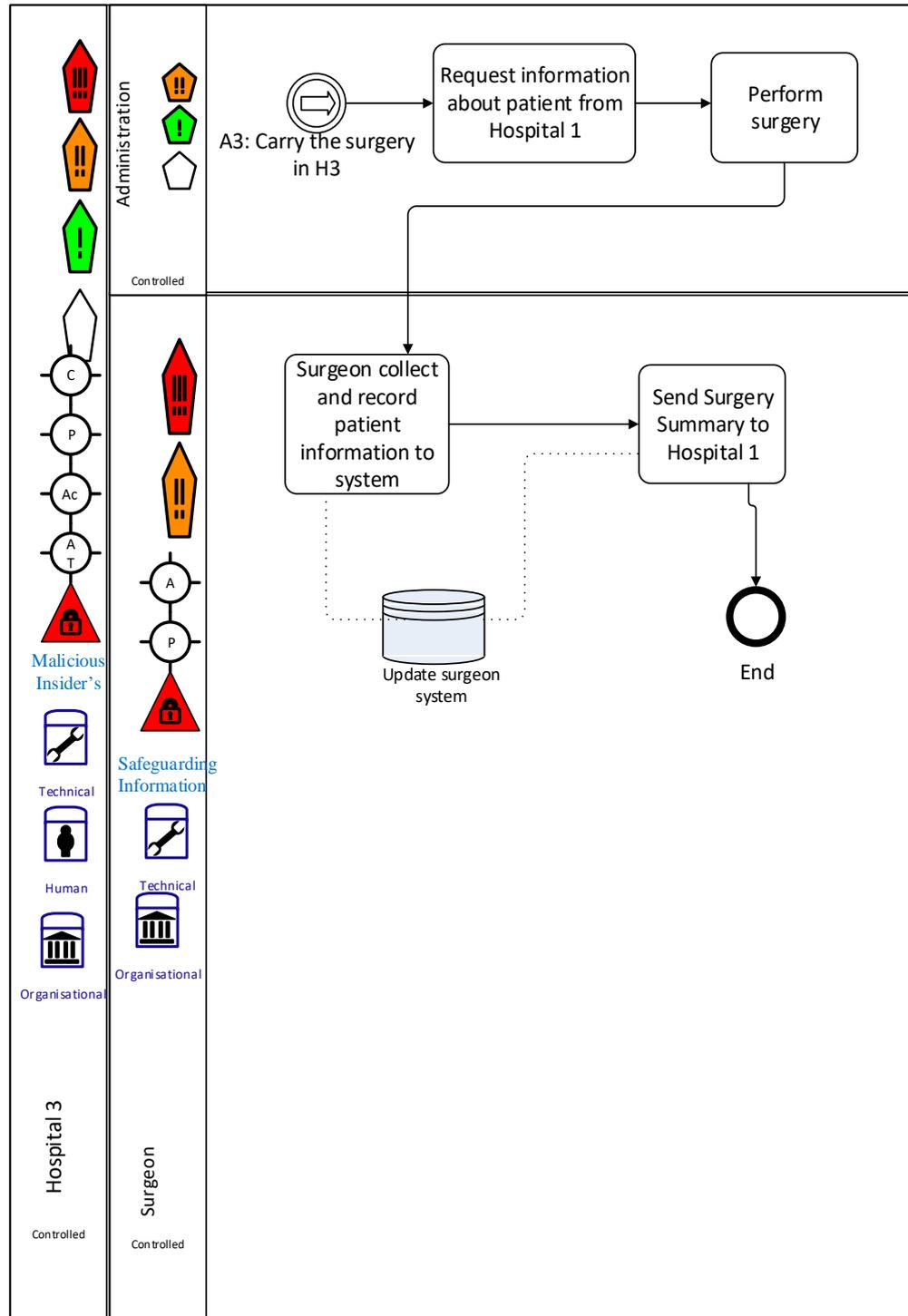
E.7 Risk Register for Patient Pathway in Hospital 2

No	Risk type	Risk Name	Impact	Likelihood	Risk Level	Security Goals	Risk Countermeasure	Traceability	Date Identified/ Modified
1	Security-15	<p>Malicious Insider's</p> <p><i>Description:</i> The risk of Hospital 2 staff members to misuse their role on the patient medical records.</p>	Very high	Medium	High	Confidentiality Privacy Accountability Authenticity & Trustworthiness	<p>Technical :specify the access control policy for each member in the Hospital 2 according to their roles and responsibilities</p> <p>Human: Hospital 2 must provide security training workshop for all members to enhance their awareness of possible threats</p> <p>Organisation: Hospital 2 has to notify all members of security policy implemented in place.</p>	<p>Process: MDT Review Meeting</p> <p>Location: Hospital 2</p>	22 Feb 2017

2	Security-6	<p>Insecure or Ineffective Deletion</p> <p><i>Description:</i> The risk of insecure or ineffective deletion of previous patient medical team or authorization for Drs to access from outside the care team.</p>	Very High	Medium	High	Privacy Integrity (accuracy)	<p>Technical : Check MDT team are within the care team and involved within the patient case to ensure the right authorisation and authentication based on their role.</p>	<p>Process: MDT Review Meeting</p> <p>Location: Hospital 2</p> <p>Rows: Insecure or ineffective deletion</p>	22 Feb 2017
3	Security-16	<p>Identity and Access Management</p> <p><i>Description:</i> The risk of involving a member outside the team care for patient case.</p>	High	Low	Medium	Confidentiality	<p>Technical: Check MDT members are involved in patient case. Need to provide authorisation and authentication to ensure the right level of access is consistent with the level of access that will become available to the user.</p>	<p>Process: MDT Review Meeting</p> <p>Location: Hospital 2</p> <p>Rows: Identity and access management</p>	22 Feb 2017

E.8 Patient Pathway in Hospital 3 with Countermeasures

Perform Surgery



E.9 Risk Register for Patient Pathway in Hospital 3

No	Risk type	Risk Name	Impact	Likelihood	Risk Level	Security Goals	Risk Countermeasure	Traceability	Date Identified / Modified
1	Security-15	<p>Malicious Insider's</p> <p><i>Description:</i> The risk of Hospital3 staff members to misuse their role on the patient medical records.</p>	Very High	Medium	High	Confidentiality Privacy Accountability Authenticity & Trustworthiness	<p>Technical :specify the access control policy for each member in the Hospital 3 according to their roles and responsibilities</p> <p>Human: Hospital 3 must provide security training workshop for all members to enhance their awareness of possible threats</p> <p>Organisation: Hospital 3 has to notify all members of security policy implemented in place.</p>	<p>Process: Perform Surgery</p> <p>Location: Hospital 3</p>	22 Feb 2017

2	Security-1	<p>Safeguarding Patient Confidential information and compliance</p> <p><i>Description:</i> The risk from Surgeon not safeguarding patient medical results and disclosure it with another person without the right approval.</p>	Very High	Medium	High	Confidentiality Accountability	<p>Technical: Surgeon needs to safeguarding patient confidential information and compliance when collecting and recording patient information in the system. He must has the right authentication and authorisation on storing medical health records and safeguarding it with key security regulations.</p>	<p>Process: Perform Surgery</p> <p>Location: Hospital 3</p> <p>Rows: Surgeon</p>	22 Feb 2017
---	------------	--	-----------	--------	------	-----------------------------------	---	--	-------------

16 Appendix F: Evaluation Methodology

F.1 Participation in a Research Evaluation

My name is Aseela Al Harthi, a PhD student at Cardiff University. My PhD Supervisors are Dr. Wendy Ivins and Prof. Omer Rana. My research is about *Managing Security Risks in Integrated Care Pathways*. I came up with an approach to assess security risks in the healthcare domain that combines Business Process Modelling with a Risk Register.

Thank you for agreeing to help with my research. Your responses and advice as a knowledgeable practitioner and/or researcher will help me evaluate our proposed approach.

The evaluation uses a healthcare scenario that has previously been applied to four PhD theses in our department. The evaluation process will involve watching a video (approximately 11 minutes) then answering questions to evaluate our proposed Security Risk Analysis and Business Process Model.

The video outlines the healthcare scenario and demonstrates how our approach can be applied to manage security risks associated with the scenario. The video covers a subset of the scenario's processes and activities so a full set of process models with their associated Risk Register has been provided for reference.

Material for evaluation:

1. URL to the Video <https://youtu.be/R0idfI9McJE>
2. Survey Questions
3. Full set of BPM and Risk Register for the healthcare scenario.

Could you please send me your completed survey via email to:
AlHarthiA@cardiff.ac.uk

If you have any questions please do not hesitate to ask me.

Best regards,

Assela

Assela Nasser Al Harthi
PhD Student at Cardiff University
Computer Science & Informatics,
Queen's Building, 5th Parade,
Cardiff, CF24 3AA
E-mail: alharthi.aseela@gmail.com or AlHarthiA@cardiff.ac.uk

F.2 Survey Questions

Survey Questions

(All information will be kept confidential and used for research purposes only. Kindly send your feedback to me on alharthia@cardiff.ac.uk or alharthi.aseela@gmail.com or to Dr. Wendy Ivins ivinswk@cardiff.ac.uk)

Part 1: Demographic Data

Q1: Your Name and Title?

Q2: Your Country?

Q3: Your role in an organisation?

Part 2: Risk Management

Q4: Your level of expertise in Risk Management or related domains?

Expert Competent Some knowledge No knowledge

If you have any experience in Risk Management or related domains, then please answer the following:

Q5: How many years of experience do you have?

Q6: What methods of Risk Management have you used?

Q7: Does your experience come from practice, research, or both?

Part 3: Business Process Models

Q8: Your level of expertise in Business Process Modeling, Business Analysis, or other related domain

Expert Competent Some knowledge No knowledge

If you have any experience in Business Process Models or related domains, then please answer the following:

Q9: How many years of experience do you have?

Q10: What methods of Business Process Modelling have you used?

Q11: Does your experience come from practice, research, or both?

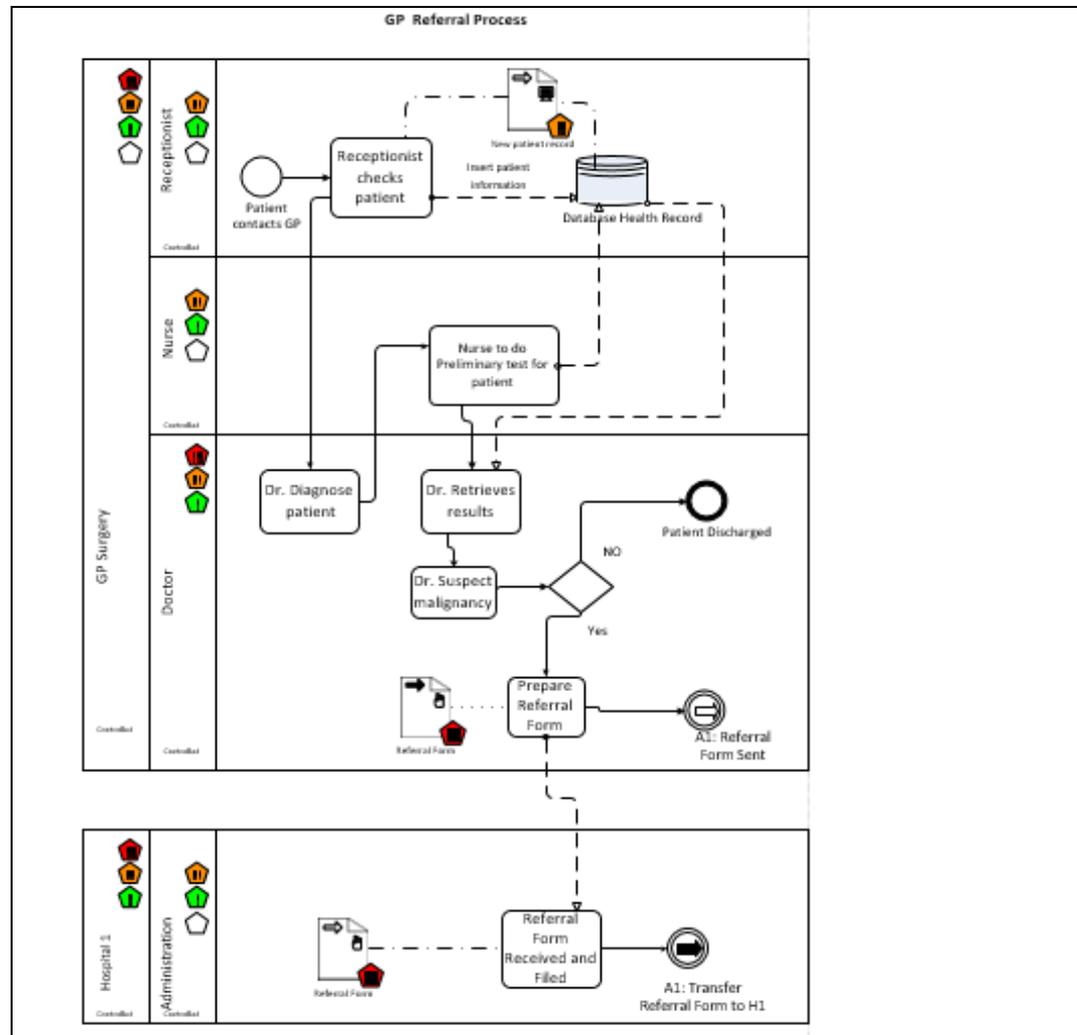
Part 4: Healthcare

Q12: Do you have experience in Healthcare or other related domain?

Q13: What is your particular area of interest/responsibility?

Part 5: Evaluation of Managing Security Risk-BPM

Stage 1: Establishing the Context : Capturing Business Process Modelling in Healthcare



Q14: The BPM approach used can be effectively applied to capture processes in healthcare.

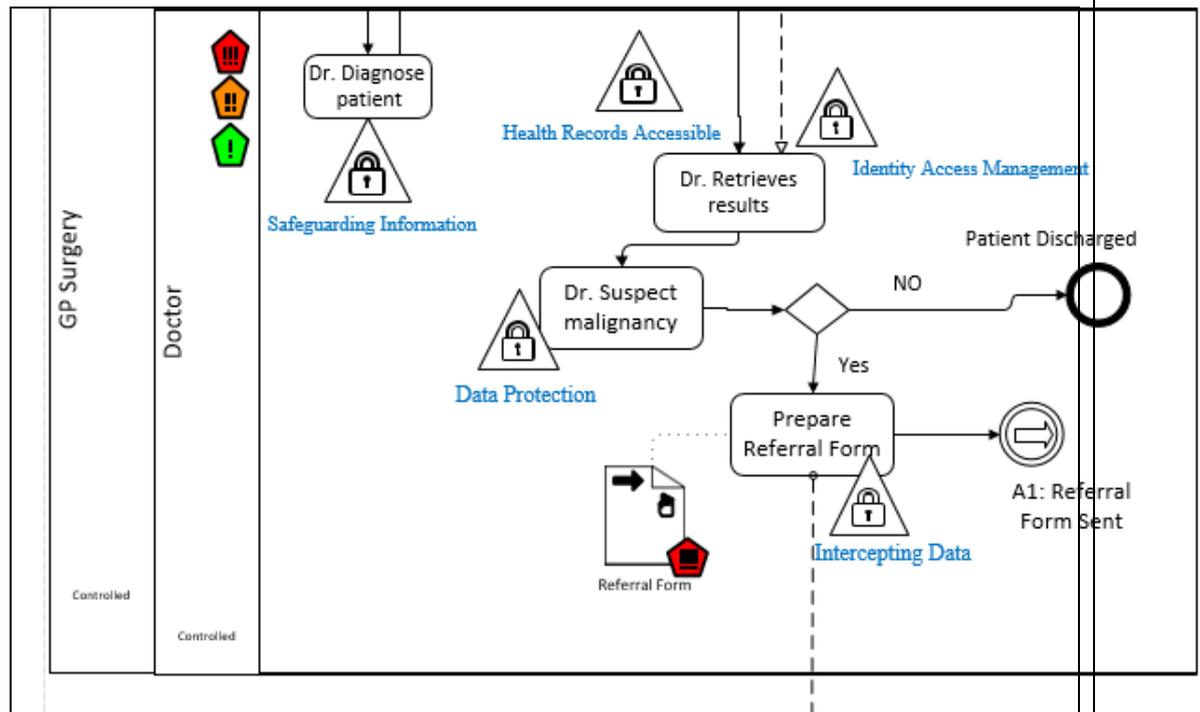
- Strongly Agree
 Agree
 Neither agree/disagree
 Disagree
 Strongly Disagree
 I do not know

Q15: The BPM approach used is useful for designing process models as it helps to clearly identify activities, flows, locations and roles in healthcare processes.

- Strongly Agree
 Agree
 Neither agree/disagree

- Disagree
- Strongly Disagree
- I do not know.

Stage 2: Identify Security Risks



Q16: The BPM approach used can clearly identify security risks with different activities level in the healthcare processes

- Strongly Agree
- Agree
- Neither agree/disagree
- Disagree
- Strongly Disagree
- I do not know

Q17: The BPM approach used is more likely to help staff identify the appropriate security risks associated with the roles compared to relying on a risk register only.

- Strongly Agree
- Agree
- Neither agree/disagree
- Disagree
- Strongly Disagree
- I do not know

Stage 3: Risk Analysis and Evaluation

No	Risk Type	Risk Name	Impact	Likelihood	Risk Level	Security Goals
5	Security-1	<p style="color: blue; margin: 0;">Safeguarding patient confidential information and compliance</p> <p>Description: The risk of Nurse disclosure patient results to someone else without the right approval during the preliminary tests conducted</p>	Very High	Medium	High	Confidentiality Accountability

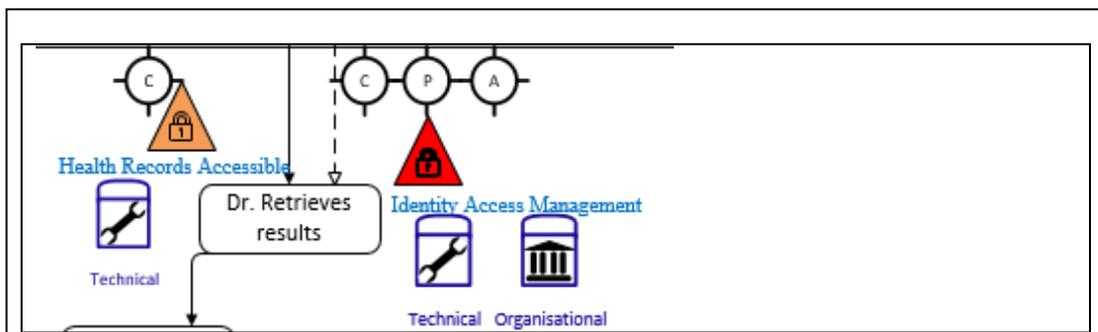
Q18: Using both the process model and risk register approach helps staff to clearly identify the appropriate security goals and risk level with each risk.

Strongly Agree
 Agree
 Neither agree/disagree
 Disagree
 Strongly Disagree
 I do not know

Q19: The Risk Register -BPM approach used is more likely to be effective in the analyses and evaluation of risk than using a risk register only.

Strongly Agree
 Agree
 Neither agree/disagree
 Disagree
 Strongly Disagree
 I do not know

Stage 4: Risk Treatment



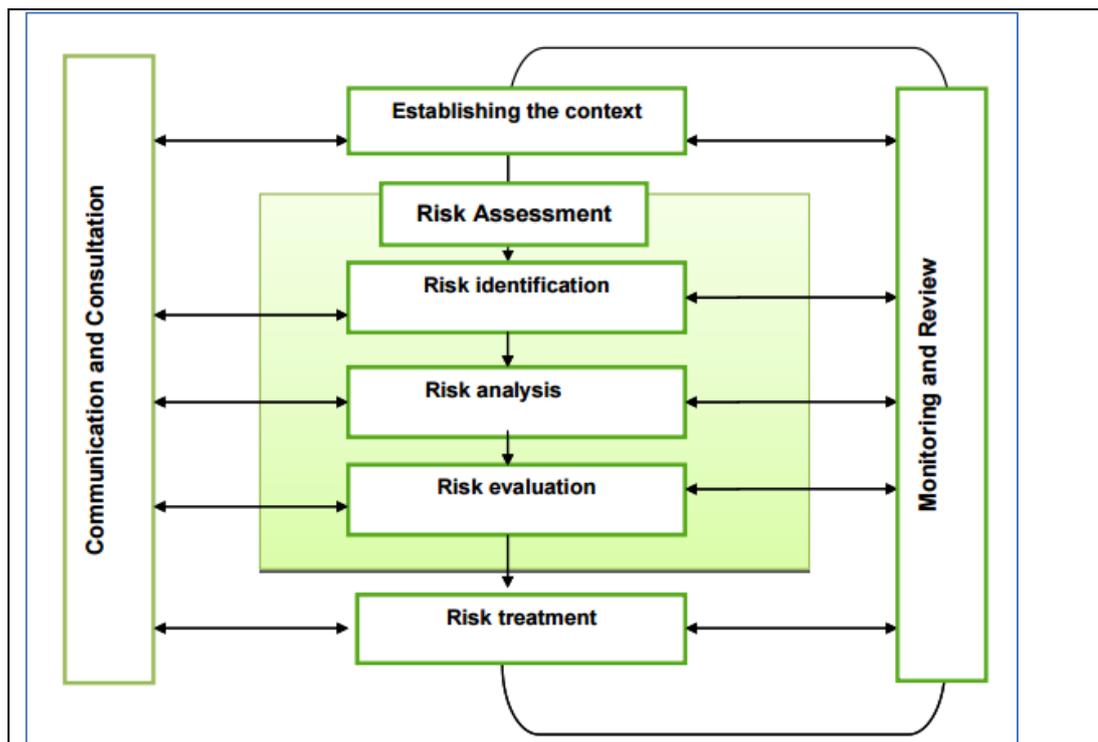
No	Risk Type	Risk Name	Impact	Likelihood	Risk Level	Security Goals	Risk Countermeasure	Traceability
6	Security-2	<p>Health records accessible</p> <p>Description: The risk of Doctor retrieves the results of another patient from health records.</p>	Very High	Medium	High	Confidentiality Privacy Availability	<p>Technical: Dr needs authorization to access and retrieves the results of a patient within his team of care as well as supporting privacy guidelines</p>	<p>Process : GP Referral</p> <p>Location GP Surgery</p> <p>Activity: Doctor Retrieves patient results</p>
7	Security-16	<p>Identity Access Management</p> <p>Description: The risk of another Doctor using identity and access privilege of another Dr. to view patient results.</p>	High	Low	Medium	Confidentiality	<p>Technical: Dr. should use registration procedure to ensure the right authorization to access and retrieves patient results is consistent with his role and identity.</p> <p>Organisational: Dr. Should follow GP policy in retrieving patient results.</p>	<p>Process : GP Referral</p> <p>Location GP Surgery</p> <p>Activity: Doctor Retrieves patient results</p>

Q20: The Risk management-BPM approach used is more likely to be effective in identifying suitable countermeasure in healthcare domain than using risk register only.

- Strongly Agree
- Agree
- Neither agree/disagree
- Disagree
- Strongly Disagree
- I do not know

Q21: Using Risk register and BPM together is more likely to help in identifying the appropriate countermeasure.

- Strongly Agree
- Agree
- Neither agree/disagree
- Disagree
- Strongly Disagree
- I do not know



Stage 5: Monitoring & Review

Q22: Using Risk register and BPM together is more likely to help in identifying any changes with the risk than using risk register only.

- Strongly Agree
- Agree
- Neither agree/disagree
- Disagree
- Strongly Disagree
- I do not know

Stage 6: Communication & Consultation

Q23: The Risk Register – BPM approach used is clearly understandable and appropriate to use to manage security risk in healthcare processes.

- Strongly Agree
- Agree
- Neither agree/disagree
- Disagree
- Strongly Disagree
- I do not know

Q24: Risk Register-BPM approach used is more likely to effectively communicate risks to achieve a shared understanding of all roles involved in the process compared to using risk register only.

- Strongly Agree
- Agree
- Neither agree/disagree
- Disagree
- Strongly Disagree
- I do not know

Q25: Developing BPM and risk register for key health processes is more likely to help healthcare organisations manage security risks in compliance to Information security risk management practices (ISO27005) compared to developing Risk register only.

- Strongly Agree
- Agree
- Neither agree/disagree
- Disagree
- Strongly Disagree
- I do not know

Other Comments:

Q26: Please outline any difficulties you may have experienced in following Risk Register-BPM approach presented in the video.

Q27: Does the Risk Register-BPM approach used include any elements that are missing or not relevant to the Managing security risks domain? If yes, please name them.

Q28: To what extent do you feel that Risk Register-BPM approach can be used as a valuable tool to complement using a risk register to manage security risks?

Q29: Do you anticipate any problems with adopting the risk register- BPM approach .if yes please provide them in details.

Q30: Any other comments or feedback?

F.3 Participant Profile Part 1

Table 1: Participant Profile Part 1

No	Country	Role in Organisation	Risk Management experience	Exper. (years)	Methods of risk Management	Nature of Exper.
P1	UK	Lecturer	Competent	6	ISO 27005, some graphical methods	Research
P2	UK	Lecturer in Safety-Critical Systems	Expert	12	Safety Methods, e.g. FMEA, FFA, HAZOP and FTA	Largely research but closely with practice (different industries)
P3	UK	Director/CTO	Competent	8	CESG's (RMADS etc.)	Practice
P4	UK	Cyber Analyst	Some knowledge	2	Risk Registers defining Treat, Transfer, Tolerate, Terminate. DREAD methodology to quantify risk, Impact x likelihood methodology to quantify risk.	Both
P5	UK	Threat Monitoring Specialist	Some knowledge	less than one year	ISO27001 & ISO31000	Postgraduate education
P6	UK	Lead Cyber Security Consultant	Some knowledge	4	Reduction and avoidance	Practice

P7	UK-Wales	Professor/Head of Workforce &OD	Competent	more than 10 years	Risk & Issues	Practice
P8	UK	Senior Sociotechnical Researcher	Competent	4	I research risk methods mainly and the use of complexity theory and risk. But I have used ISO27001 and bits of IS1&2, Cynefin (sensemaking tool)	Mainly research these days
P9	UK-England	Cyber Security Customer Solutions Architect	Some knowledge	2	Specifically: ISO 27001 implementation, PCI DSS implementation, Internal Risk Pro project management toolsets Alongside: Vulnerability analysis. ISMS implementation. Contractual risk analysis (for acceptable risks). Disaster recovery / continuity planning. Business process modelling / planning to adapt Audit criteria and processes to manage risk and comply with risk management requirements. Academic: • Cardiff MSc thesis on securing virtualized infrastructures / deployments within an IaaS environment. Focus was on technical, operational and life cycle security.	Mainly practise, some theoretical knowledge from Academic studies (see above).

					<ul style="list-style-type: none">• Risk Management covered within SSCP & CISSP Certifications	
P10	UK-Wales	Clinical Fellow (Junior Dr); Previously Project Support Manager, NHS Wales Informatics Service	Some knowledge	5 years	PRINCE methodology	Practice

P11	UK	Cyber Sales Executive	Competent	6	Primarily Risk Registers when used during system design and specification. These are usually customer supplied and a typical requirement would be to state mitigation measures against the stated risks.	Mainly practice but also related study also supervised by Wendy.
P12	UK-England	Cybersecurity Director - Lead cyber security and cyber insurance (including risk assessment)	Expert	7	Qualitative, Quantitative, ISO27000, various supply chain methodologies, government methodologies (IS1/IS2), bespoke methodologies, US Federal methodologies, regulatory/standards-based methodologies (ISA99, CFATS, safety cases etc)	Practice

F.4 Participant Profile Part 2

Participant Profile Part 2

No	BPM Experience	Exper. (years)	Methods of BPM	Nature of Exper.	Healthcare Experience	Area of interests /responsibility
P1	Competent	6	BPMN	Research	No	N/A
P2	Competent	3	BPMN, activity diagrams and flowcharts	Largely research but closely with practice (different industries)	Yes	Research and engineering in patient safety
P3	Expert	10	UML, BPMN, MODAF	Practice	Yes	Was electronic health records in oncology and evidence-based medicine
P4	Some knowledge	less than 1	BPMN	Research	N/A	N/A
P5	Some knowledge	3	Flowcharts, Swimlane, Data Flow Diagrams	Both	No	Cyber Security Attacks and Investigations
P6	Some knowledge	4	UML, Flowchart, GANTT	Practice	No	No

P7	Competent	more than 10 years	Process mapping/business modelling	Practice	IT arm of the NHS	Head of Workforce but lead the national team of service transformation
P8	Some knowledge	4	Soft Systems Methodology, System Dynamics, SABSA,	Mainly research	Yes	I used to work in IT in the NHS and its comes up as an area of research now especially with the growth of IoT.
P9	Some knowledge	9 months	Acting Service architect covering business process reengineering utilized: <ul style="list-style-type: none"> • Swim lanes • Data flow diagrams • UML Diagrams • Some role activity diagram 	· Practise (with the exception of Dr Wendy Ivins MSc Classes)	No	Cyber: Networks, Virtualization, Cloud, PKI, SIEM. Recent experience with risk analysis and vulnerability analysis, some service design exposure and business process engineering in current role alongside being a PKI SME.
P10	Some knowledge	5 years	Soft systems methodology	Both	Yes	Health Informatics
P11	Competent	6	MODAF, EA, UML, SSM, SD. I appreciate that some of these are tools and some are methods.	Mainly practice from the level of managing risk management practitioners as part of an Integrated Project Team.	No. My experience is in Defence and Government Agency.	I am the lead account manager for NATO CIRC and am also leading another project to deliver large scale cyber defence to a major EU Agency. I am involved in all aspects

						of deploying cyber defence systems at scale which typically include consult, design, build and operate functions.
P12	Competent	5	UML, OO methods, flow charts, work flow, role interaction	Research	Yes	UK healthcare (NHS), Insure multiple entities in the US for all healthcare related cyber risk (as covered under HIPAA/HITECH).

F.5 Participant Feedback for Q14 to Q25

No	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25
P1	Agree	Strongly Agree	Strongly Agree	Agree	Strongly Agree	Strongly Agree	Neither agree/disagree	Neither agree/disagree	Strongly Agree	Agree	Strongly Agree	Agree
P2	Agree	Agree	Agree	I do not know	Neither agree/disagree							
P3	Agree	Strongly Agree	Neither agree/disagree	Agree	Agree	Agree	Agree	Agree	Strongly Agree	Disagree	Agree	Agree
P4	Agree	Agree	Agree	Strongly Agree	Agree	Agree	Agree	Disagree	Agree	Agree	Strongly Agree	Agree
P5	Agree	Agree	Agree	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree	Neither agree/disagree	Agree	Agree	Agree
P6	Agree	Strongly Agree	Agree	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree
P7	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
P8	Agree	Agree	Agree	Agree	Neither agree/disagree	Agree	Agree	Neither agree/disagree	Agree	Agree	Agree	Agree

P9	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree	Strongly Agree	Strongly Agree
P10	Agree	Agree	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	I do not know
P11	Agree	Agree	Agree	Agree	Strongly Agree	Strongly Agree	Disagree *	Disagree *	Strongly Agree	Agree	Strongly Agree	Agree
P12	Agree	Agree	Neither agree/disagree	Disagree	Agree	Agree	Neither agree/disagree*	Neither agree/disagree*	Agree	Neither agree/disagree	blank	blank

F.6 Participant Feedback for Q26- Q30

Feedback from Participant 1

Other Comments:

Q26: Please outline any difficulties you may have experienced in following Risk Register-BPM approach presented in the video.

I followed the method easily. My main concern is that the final annotated diagram is overcrowded with symbols which make reading and understanding harder. I would suggest that in future work you should consider how to improve the effectiveness of the visual representation of annotated BPMN models.

Q27: Does the Risk Register-BPM approach used include any elements that are missing or not relevant to the Managing security risks domain? If yes, please name them.

Privacy is critical in healthcare, but at the same time data are collected for important medical analysis. So you may want, in future work, to consider representation or privacy and address issues of data anonymization.

Q28: To what extent do you feel that Risk Register-BPM approach can be used as a valuable of tool to complement using a risk register to manager security risks?

If used appropriately, the method could bring multiple benefits as it helps to visualise security risks in complex business processes, and make them explicit and easy to see for experts with different backgrounds.

Q 29: Do you anticipate any problems with adopting the risk register- BPM approach .if yes please provide them in in details.

As this is not a standardised or widely used method, I anticipate a lot of difficulties with adopting a method in large and heavily regulated organisations. The method would have to go through a lot of empirical testing, and several rounds of evaluation and improvement before it may be adopted in practice.

Q30: Any other comments or feedback?

Regarding Q20 and Q21, I do not see how this method could actually help with identifying appropriated countermeasures. They could be equally well identified based on the description of the problem provided in a risk register. It only depends on how detailed is the register and how detailed is a model. Although, I can clearly see the benefits of the method for structuring and organising risk related information, I am not sure that it assists with identifying countermeasures. If in future work, you could extend the method do that it provides some

automated recommendations for similar risks, then it potentially may be helpful for this purpose as well.

Feedback from Participant 2

Other Comments:

Q26: Please outline any difficulties you may have experienced in following Risk Register-BPM approach presented in the video.

Who is the user of your approach? A security engineer or a clinician? I would say an engineer might be familiar with this sort of modelling. I doubt a clinician will have the skill or time to develop these models.

Q27: Does the Risk Register-BPM approach used include any elements that are missing or not relevant to the Managing security risks domain? If yes, please name them.

As a framework it's fine. The problem is in having data/evidence to decide on things like likelihood and impact parameters.

Q28: To what extent do you feel that Risk Register-BPM approach can be used as a valuable tool to complement using a risk register to manage security risks?

The value lies in improving traceability between the technology and the clinical setting.

Q 29: Do you anticipate any problems with adopting the risk register- BPM approach .if yes please provide them in details.

User acceptance might be an issue, especially if the intended user is not an engineer, e.g. doctor or nurse.

Q30: Any other comments or feedback?

It was hard to answer your questions since you do not provide a reference/benchmark against which to compare your approach. For example, is it nothing vs your approach? Or using flowchart vs BPMN? This makes a big difference.

Feedback from Participant 3

Other Comments:

Q26: Please outline any difficulties you may have experienced in following Risk Register-BPM approach presented in the video.

Followed fine

Q27: Does the Risk Register-BPM approach used include any elements that are missing or not relevant to the Managing security risks domain? If yes, please name them.

Q28: To what extent do you feel that Risk Register-BPM approach can be used as a valuable of tool to complement using a risk register to manager security risks?

It's better than just a risk register but I haven't seen it compared to CESGs approach to infosec risk management – which as a public sector body they should adhere to – hence harsh mark on Q23 – sorry – search google on GPMS and RMADS (risk management and accreditation documents set) if you are unsure – this will start you down the right route

Q 29: Do you anticipate any problems with adopting the risk register- BPM approach .if yes please provide them in in details.

See above – would be fine but as part of a wider RMADS / approach to implementing GPMS – basically needs lots of scoping documents and quite a lot of other stuff – after recent events this is likely to be pretty important

Q30: Any other comments or feedback?

Good luck

Feedback from Participant 4

Other Comments:

Q26: Please outline any difficulties you may have experienced in following Risk Register-BPM approach presented in the video.

Does Hospital 1,2,3 infer that for each cancer diagnosis, three separate hospitals are used each time?

Q27: Does the Risk Register-BPM approach used include any elements that are missing or not relevant to the Managing security risks domain? If yes, please name them.

-

Q28: To what extent do you feel that Risk Register-BPM approach can be used as a valuable tool to complement using a risk register to manage security risks?

Certainly more readable, understandable and referable than a potentially large and unwieldy risk register.

Q 29: Do you anticipate any problems with adopting the risk register- BPM approach .if yes please provide them in details.

It would depend on how process varies across hospital 'constituencies' in the UK – is the process totally standardised across all hospitals? (I don't know the answer to that)

Q30: Any other comments or feedback?

I would assume that the same actors highlighted in the above BPM's are also responsible for data at rest, would this be included in the above process?

Feedback from Participant 5

Other Comments:

Q26: Please outline any difficulties you may have experienced in following Risk Register-BPM approach presented in the video.

No difficulties to mention.

Q27: Does the Risk Register-BPM approach used include any elements that are missing or not relevant to the Managing security risks domain? If yes, please name them.

Although I quite liked the model and is a great starting point to evaluate risk, I think it might be missing the following points:

- **Physical Access:** The actors have been defined in the swim-lanes have neglected the outsider threat or any actor that is not part of the process. Such as can somebody walk-in and access the system? What physical access controls are available from stopping them? How about a break-in?
- **Data at rest:** In your diagram, you did mention a database of health records, but I think a bit more detail is required here; Firstly, for the point I mentioned above (physical access). Secondly the technical aspects of protecting the data (type of encryption used, etc.) and lastly, to address availability and continuity; Is this a single point of failure? Is there a hot/warm site available in case of disaster?

Q28: To what extent do you feel that Risk Register-BPM approach can be used as a valuable of tool to complement using a risk register to manager security risks?

As I mentioned earlier, I quite liked the model and is a great starting point to evaluate risk particularly when establishing processes.

Q 29: Do you anticipate any problems with adopting the risk register- BPM approach .if yes please provide them in in details.

The only problem I can think of is that most organisations already have a risk template that they follow with different level schema, which could involve a lot of levels (A1,A3, B3, etc.) and it might be difficult to map their existing schema with the three levels (Red, Amber and Green)

Q30: Any other comments or feedback?

Nope.

Feedback from participant 6

Other Comments:

Q26: Please outline any difficulties you may have experienced in following Risk Register-BPM approach presented in the video. **None, you explain it clearly.**

Q27: Does the Risk Register-BPM approach used include any elements that are missing or not relevant to the Managing security risks domain? If yes, please name them. **Not that I noticed, but this isn't my domain of expertise.**

Q28: To what extent do you feel that Risk Register-BPM approach can be used as a valuable of tool to complement using a risk register to manager security risks? **Have the right methodology and tooling is essential for managing security risk. Having a methodology that is sound is good, and I think this can be used, but you would need to spend the time not just creating the method but also building the training and implementation capability, as people performing this work are incredibly busy and don't always have time to learn new methods if the methods they are using are 'good enough' Being a better method is not always a good enough reason to stop doing what has been working, so you'll need to construct a compelling reason not just why this is good, but also why the current method is not good.**

Q 29: Do you anticipate any problems with adopting the risk register- BPM approach .if yes please provide them in in details. **What I mentioned above. It's hard in busy spaces, especially in health care, to learn and use new things. This would have to be used by multiple practitioners in different hospitals for it to be effective, with the underlying DB constructed in a way to collect the right information, so to make this effective it's not just convincing one manager or one hospital, but a group of them working together. Is there a need for this in the marketplace? Do hospitals see a problem with what they are using to demand something better?**

Q30: Any other comments or feedback?

Feedback from Participant 7

Other Comments:

Q26: Please outline any difficulties you may have experienced in following Risk Register-BPM approach presented in the video.

Q27: Does the Risk Register-BPM approach used include any elements that are missing or not relevant to the Managing security risks domain? If yes, please name them.

Q28: To what extent do you feel that Risk Register-BPM approach can be used as a valuable tool to complement using a risk register to manage security risks? To a great extent

Q 29: Do you anticipate any problems with adopting the risk register- BPM approach .if yes please provide them in details. No

Q30: Any other comments or feedback?

Feedback from Participant 8

Other Comments:

Q26: Please outline any difficulties you may have experienced in following Risk Register-BPM approach presented in the video.

I would be cautious with your examples and their ratings, people have a tendency to just copy by default what has gone before in the examples, as they stick with the defaults. Taking this into account for your examples would be quite helpful as I would question the levels of impact associated with certain parts of this, is a malicious insider across the NHS process really a medium likelihood?

Also what does malicious insider mean in a hospital sense? It might be worth looking at this piece of work <https://www.crestresearch.ac.uk/csrfliipbook/issue-2/?page=10>

What does High, Medium and low mean?

Q27: Does the Risk Register-BPM approach used include any elements that are missing or not relevant to the Managing security risks domain? If yes, please name them.

There is a move with risk to the use of complexity theory, especially in the areas like sensemaking. It might be worth taking a look at these things. This is an interesting paper

<http://dl.acm.org/citation.cfm?id=2841119>

Q28: To what extent do you feel that Risk Register-BPM approach can be used as a valuable tool to complement using a risk register to manage security risks?

I think it is useful to have the visualisation for people so they can see the connections across an organisation and the flow. This is often what is missing a lot of the time.

Q 29: Do you anticipate any problems with adopting the risk register- BPM approach .if yes please provide them in details.

As mentioned above I would question the time and capacity people have to do this. They are often stretched for time, why would they adopt this over just keeping with the risk register? As much as its known risk registers aren't the best and have many issues, how will you bring people with you, to make them understand what could be done with this work?

Q30: Any other comments or feedback?

Feedback from participant 9

Other Comments:

Q26: Please outline any difficulties you may have experienced in following Risk Register-BPM approach presented in the video.

None

Q27: Does the Risk Register-BPM approach used include any elements that are missing or not relevant to the Managing security risks domain? If yes, please name them.

Q28: To what extent do you feel that Risk Register-BPM approach can be used as a valuable tool to complement using a risk register to manage security risks?

I feel it is of significant value in comparison to a traditional risk register. If this was applied in detail to a very specific hospital / health care facility, it could be used as starting point to understand risk, referencing out to more detailed documents to form a holistic risk analysis. If this were updated as departmental processes evolve, it could be used to inform the 'plan' aspect of a health care providers ISMS.

Q 29: Do you anticipate any problems with adopting the risk register- BPM approach .if yes please provide them in in details.

No

Q30: Any other comments or feedback?

None, keep up the good work :)

Feedback from Participant 10

Other Comments:

Q26: Please outline any difficulties you may have experienced in following Risk Register-BPM approach presented in the video.

None

Q27: Does the Risk Register-BPM approach used include any elements that are missing or not relevant to the Managing security risks domain? If yes, please name them.

None

Q28: To what extent do you feel that Risk Register-BPM approach can be used as a valuable tool to complement using a risk register to manage security risks?

It is useful in explaining the underlying process and in my opinion stakeholders will find it helpful to view the exact points/processes which have underlying risks.

Q 29: Do you anticipate any problems with adopting the risk register- BPM approach .if yes please provide them in details.

None

Q30: Any other comments or feedback?

This model of three different hospitals may not be a universal model but it will be applicable in few scenarios. There would be some patient who will go from GP to Hospital 1 (usually holds the first and subsequent MDTs) for further assessment and then Hospital 2 for treatment (Hospital 2 will hold MDTs as well).

But the scenario is a very practical one and associated risks are better identified using the BPM and risk register approach. Well done.

Feedback from participant 11

Other Comments:

Q26: Please outline any difficulties you may have experienced in following Risk Register-BPM approach presented in the video.

Q27: Does the Risk Register-BPM approach used include any elements that are missing or not relevant to the Managing security risks domain? If yes, please name them.

I am currently engaged in the design of a cyber security monitoring system for a major EU agency and we are using an approach which tries to capture the information you have captured here using an EA / MODAF / UML based method. One of the things that we have found to be very useful is to take into consideration the customer 'Feared Events'. These tend to be high level and help people to think about the risks without the constraints of current infrastructure / people / process / technology. It also helps in stopping people 'solutionising' (sorry – horrible word) too early in the process. This type of approach also helps people consider the risks introduced by process and people, as opposed to being purely technology focussed, which is a real problem in my experience. It is important for the security system design team to understand where the risks are derived from so that they can be effectively mitigated in the solution. Another useful question is to identify the organisations 'crown jewels' so that you know what is of most value to the customer. It is always useful to gain as many perspectives from as many different sources as practical.

Q28: To what extent do you feel that Risk Register-BPM approach can be used as a valuable tool to complement using a risk register to manage security risks?

I think it would be an improvement on what currently exists. We are often presented with a risk register during consult / system design phases which tend to be a cut and paste of the last one with no real thought into the actual risk. It would be more likely to be a living document than a risk register which tends to be ignored after the initial project implementation.

Q 29: Do you anticipate any problems with adopting the risk register- BPM approach .if yes please provide them in details.

The supporting functions such as training and system management of implementing such a system at scale should not be underestimated. Systemic change is always difficult. Typically, the change management function within the organisation would look after the living document so system change in that area would be required.

Q30: Any other comments or feedback?

I always find modelling to be very useful and I like the way that the BPM is linked to the register. Maintaining this link would be quite difficult though and would need change / configuration management to ensure successful use. To be effective it would also need to be

linked to the security system design documentation to measure how well the identified risks are mitigated (or not) as the systems capability (in terms of people, process and technology) change over time.

Feedback from Participant 12

Other Comments:

Q26: Please outline any difficulties you may have experienced in following Risk Register-BPM approach presented in the video.

None

Q27: Does the Risk Register-BPM approach used include any elements that are missing or not relevant to the Managing security risks domain? If yes, please name them.

Yes - it is hard to list but is also equally difficult because it is a question of semantics, definitions and your underlying goal. Typically this approach will enable the identification of risks through a particular lens - in this case a process. However security is somewhat all encompassing. Depending on the ultimate consumer of the activity, sticking to this approach will likely miss more binary risks driven by regulatory compliance; technical risk driven by more extensible systems and architectures (eg cloud infrastructure not managed by you) as well as contractual risk. I don't know the overall objective so it's hard to contextualise the question, so it may be appropriate, alternatively a broader approach may be required whereby this assessment can be used as part of a number of techniques to derive the overall risk posture.

Q28: To what extent do you feel that Risk Register-BPM approach can be used as a valuable of tool to complement using a risk register to manager security risks?

It will be a helpful tool in identifying some risks through a logical process flow, however it shouldn't be used in isolation. Equally, risk registers are used for simplicity and the ability of a wide audience to be able to consume their outputs and contribute. It's possible that whilst this is good for a technical audience, you may have security risks that threaten brand or more nebulous economic value. It's likely stakeholders you'd want to engage in this process won't be from a technical background and may struggle conceptually with it, so alternative techniques may be required.

Q 29: Do you anticipate any problems with adopting the risk register- BPM approach .if yes please provide them in in details.

See above. S

Q30: Any other comments or feedback?