

This is an Open Access document downloaded from ORCA, Cardiff University's institutional repository: <https://orca.cardiff.ac.uk/id/eprint/181867/>

This is the author's version of a work that was submitted to / accepted for publication.

Citation for final published version:

Alotaibi, Maha, Cherdantseva, Yulia and Teehan, Catherine 2026. Methodology for designing and developing a cybersecurity curriculum for secondary schools. Presented at: 7th International Conference on Blockchain Computing and Applications (BCCA), Durbovnic, Croatia, 14-17 October 2025. 2025 7th International Conference on Blockchain Computing and Applications (BCCA). IEEE Xplore Digital Library. IEEE, pp. 926-934. 10.1109/BCCA66705.2025.11227168

Publishers page: <https://doi.org/10.1109/BCCA66705.2025.11227168>

Please note:

Changes made as a result of publishing processes such as copy-editing, formatting and page numbers may not be reflected in this version. For the definitive version of this publication, please refer to the published source. You are advised to consult the publisher's version if you wish to cite this paper.

This version is being made available in accordance with publisher policies. See <http://orca.cf.ac.uk/policies.html> for usage policies. Copyright and moral rights for publications made available in ORCA are retained by the copyright holders.



Methodology for Designing and Developing a Cybersecurity Curriculum for Secondary Schools

Maha Alotaibi
Computer Science and Informatics
Cardiff University
Cardiff, UK
AlotaibiM11@cardiff.ac.uk
0009-0002-5687-4308

Yulia Cherdantseva
Computer Science and Informatics
Cardiff University
Cardiff, UK
CherdantsevaYV@cardiff.ac.uk
0000-0002-3527-1121

Catherine Teehan
Computer Science and Informatics
Cardiff University
Cardiff, UK
teehanc@cardiff.ac.uk
0000-0002-2359-0694

Abstract—The extensive implementation of digital technologies has introduced significant cybersecurity risks for secondary school students, revealing major deficiencies in structured instruction, teacher preparation, and institutional support. From 2022 to 2024, a study conducted across Welsh secondary schools established a systematic methodology for cybersecurity curriculum design and development based on the Design Science Research Methodology (DSRM). The approach integrates five key cybersecurity knowledge areas and pedagogical frameworks, including the Cyber Security Body of Knowledge (CyBOK) and the Digital Competence Framework, into a structured curriculum supported by technological tools for customization.

This paper presents the DSRM-based methodology developed to address the lack of standardized cybersecurity education and the challenges of teacher preparation. As part of a broader research project, this work focuses on the methodological framework; empirical evaluation of its effectiveness will be reported in future publications. The paper concludes with recommendations on implementation, scalability, and ongoing development, emphasizing the potential for global adoption and the need for sustained institutional commitment to cybersecurity education.

Index Terms—cybersecurity curriculum, cybersecurity education, secondary school education, curricular gaps.

I. INTRODUCTION

The extensive integration of digital technology has significantly transformed society, particularly affecting secondary school students who are increasingly vulnerable to sophisticated cyberattacks [1]. Recent statistics indicate that nine out of ten young Europeans access the Internet daily [2]. While adolescents benefit from online communication and information sharing, they are also exposed to various risks, including privacy breaches, identity theft, malware infections, and unauthorized financial activity [2]. Therefore, it is essential that school curricula incorporate cybersecurity education to equip younger generations with the knowledge and skills required to recognize significant online risks and adopt

responsible behaviors that minimize exposure to digital threats [2]–[5].

Challenges in teaching and learning cybersecurity at the school level primarily relate to teachers' limited knowledge, confidence, and resources. Cybersecurity is not systematically taught in most K–12 settings [6]. Studies show that many teachers responsible for informatics subjects have never studied cybersecurity, either as a standalone discipline or as part of computer science education [7], [8]. Consequently, teachers often lack a basic understanding of cybersecurity, leading to low confidence in teaching the subject. This issue is particularly evident among educators without a technical background or prior exposure to cybersecurity concepts, resulting in hesitation and uncertainty about integrating such content into their curricula. In addition, teachers frequently report feeling unprepared to deliver effective cybersecurity instruction due to insufficient training and outdated materials [9]. Educators also note that existing curricula are inconsistent and that they struggle to find engaging, practical resources aligned with students' needs and current cybersecurity standards [7].

Research highlights that the lack of cybersecurity education represents a global concern, with estimates suggesting that it may take up to two decades to close the current competency gap across educational institutions at all academic levels [10]. Addressing this gap requires the establishment of comprehensive educational pathways that develop essential skills for navigating an increasingly digital society. Early exposure to cybersecurity concepts not only creates a pipeline of future cybersecurity professionals but also fosters critical digital literacy skills that help protect individuals and communities from emerging cyber threats [5].

This paper presents a methodology for designing a comprehensive cybersecurity curriculum framework as part of a larger research project on cybersecurity ed-

education in secondary schools. Specifically, it focuses on the systematic design and development phases of curriculum creation using the Design Science Research Methodology (DSRM) as the foundational approach. The primary contribution of this work is the introduction of a novel methodology that combines DSRM with curriculum mapping techniques to address the identified deficiencies in cybersecurity education. While this paper focuses on the methodological framework, empirical evaluation through teacher focus groups and implementation trials will be reported in future publications.

The primary contribution of this paper is the presentation of a novel methodology that combines DSRM with curriculum mapping techniques to address the identified gaps in cybersecurity education. While this paper focuses exclusively on the methodological framework design, the empirical evaluation of the framework's effectiveness through focus group evaluation with teacher and implementation trials will be reported in future publications.

The remainder of this paper is organized as follows. Section II reviews related work. Section III describes the Design Science Research Methodology (DSRM) applied to the design and development of the cybersecurity education program for secondary schools. Section IV presents the proposed curriculum design methodology and its implementation process. Section V discusses the key findings, implications, and limitations of this work. Finally, Section VI concludes the paper and outlines directions for future research.

II. BACKGROUND AND RELATED WORK

The growing recognition of cybersecurity as a multidisciplinary field spanning computer science, education, policy, and the social sciences has prompted the development of numerous educational frameworks and approaches [11], [12]. Several foundational frameworks have been introduced to guide the design of cybersecurity education. For example, Bhatia *et al.* (2023) demonstrated the effectiveness of problem-based learning in ethical hacking and network defense curricula, showing that hands-on problem-solving enhances student engagement and practical skill development [13].

From a methodological perspective, Kim and Beuran (2018) proposed a comprehensive six-step model for designing cybersecurity education programs in higher education, emphasizing the need to review existing curricula, define learning frameworks, and iteratively test them in authentic classroom environments [14]. Their work underscores the importance of tailoring educational designs to institutional contexts, learner needs, and industry expectations, providing a flexible model applicable across diverse settings.

Costa *et al.* (2023) examined gender-inclusive approaches to cybersecurity education, identifying effective methods for engaging high school girls and addressing

participation disparities in the field [3]. Their findings highlight the importance of inclusive pedagogical strategies that engage diverse student populations in cybersecurity learning. In parallel, the use of gamification and interactive learning technologies has received considerable attention. Adams and Makramalla (2017) introduced attacker-centric gamified learning environments for cybersecurity training, demonstrating how simulation-based methods can prepare students for real-world security challenges [4]. Such experiential approaches align with broader educational trends that bridge the gap between theoretical understanding and practical application.

Despite these advances, research on the current state of cybersecurity education continues to reveal significant implementation gaps. Tsado (2019) argues for institution-wide, multidisciplinary approaches to cybersecurity education, emphasizing that successful implementation depends on strategic leadership and cross-curricular integration rather than isolated instructional units [15], [16]. These insights underscore the continuing need for comprehensive educational frameworks that address both curriculum design and teacher preparation within secondary education.

III. METHODOLOGY FOR DESIGNING AND DEVELOPING CYBERSECURITY CURRICULUM FOR SECONDARY SCHOOLS

Educational curriculum design is inherently complex. One of the primary objectives of this work was to simplify the process to facilitate the development of cybersecurity curricula for the secondary school level. Simplifying this process expands the scope of cybersecurity education to address the needs of educational institutions, teachers, students, industry, and the broader global community.

The proposed methodology for cybersecurity curriculum design involves three main stages: establishing an educational framework, selecting appropriate pedagogical methods, and developing the corresponding educational content. This structured methodology was developed using the Design Science Research Methodology (DSRM) as the guiding framework, ensuring both theoretical rigor and practical applicability.

A. Overview of design science research methodology

The Design Science Research Methodology (DSRM) is a structured approach used to develop technology-based solutions that address real-world problems effectively [17]. In recent years, DSRM has been widely adopted across multiple disciplines, including cybersecurity. As digital technologies advance and the frequency of cyberattacks increases, the need for innovative and practical cybersecurity solutions has become more critical. Consequently, researchers have applied DSRM as

a framework for designing, developing, and evaluating effective solutions within the cybersecurity domain [18].

DSRM consists of a sequence of six iterative steps. A brief description of each step is provided below [19].

Step 1: Problem Identification and Motivation: Define the problem and justify the relevance of its solution. This step emphasizes the significance of the issue and identifies weaknesses in existing solutions.

Step 2: Define the Objectives of the Solution: Determine how the identified problem can be addressed. General objectives such as feasibility and performance are established, along with specific goals that guide the solution design.

Step 3: Design and Development: Develop an artifact—such as a model, framework, method, or technology that provides a potential solution to the defined problem.

Step 4: Demonstration: Demonstrate the functionality of the artifact by applying it to one or more instances of the problem to verify its practical relevance.

Step 5: Evaluation: Observe and measure the artifact's performance in solving the problem. Assessment criteria may include effectiveness, efficiency, and applicability.

Step 6: Communication: Disseminate the results and contributions of the research to relevant academic, professional, and practitioner communities.

IV. APPLYING DSRM TO CYBER SECURITY CURRICULUM DESIGN

This section presents the DSRM methodology framework as applied to our cybersecurity curriculum design context, aiming to improve cybersecurity teaching and learning approaches and ensure that most teachers can acquire fundamental cybersecurity knowledge and skills. The overall process for defining the objectives and scope of the cybersecurity curriculum methodology is illustrated in Figure 1.

A. Step 1: Problem identification and motivation

This step is crucial for identifying current challenges in cybersecurity education for secondary school students. The process involved a comprehensive literature review and structured interviews with teachers to capture both theoretical and practical perspectives.

The literature review, as detailed in [20], systematically examined existing studies, educational standards, and curricula to identify the key areas of cybersecurity knowledge typically addressed in secondary education. The review incorporated multiple sources, including established frameworks such as the Cyber Security Body of Knowledge (CyBOK) [21]. A comparative analysis of twelve international computer science curricula was also conducted to understand global approaches to cybersecurity integration and to identify best practices across different educational systems [20].

The findings revealed the absence of a standardized cybersecurity framework for secondary education worldwide and highlighted the urgent need for a consistent, structured program that addresses knowledge gaps and provides teachers with the professional development and instructional resources required for effective cybersecurity pedagogy [20].

In addition to the literature review, a thematic analysis was performed using data collected from structured interviews with twenty-seven secondary school teachers representing both technical and non-technical backgrounds [7]. The results confirmed persistent implementation challenges that align with prior studies on cybersecurity education inadequacies [12], [22]. A recurring theme was the lack of professional development opportunities, which led to low teacher confidence in content delivery, as well as the scarcity of practical teaching resources that connect theoretical concepts to real-world applications.

In summary, the identified problems in current secondary school cybersecurity education include: (1) the absence of a standardized framework, resulting in inconsistent instructional practices across educational systems, and (2) insufficient teacher training and resource provision, which together hinder the effective implementation of cybersecurity curricula.

B. Step 2: Define the objectives of a solution

Based on the findings from the previous step, it was determined that a structured methodology is required to design and develop a cybersecurity curriculum that effectively bridges the gaps in current cybersecurity education. This step synthesizes insights from the comprehensive literature review and teacher interviews to define the scope and objectives of the proposed curriculum design methodology.

The process involved adapting the knowledge areas defined in the (CyBOK) framework [23] and integrating methodological principles from the CONCORDIA framework, which provides guidelines for developing cybersecurity courses and instructional materials for professionals [24]. By combining these approaches, a tailored methodology was developed to guide the design and implementation of an educational model suitable for secondary education.

The resulting framework was structured to enhance both teachers' and students' cybersecurity knowledge through pedagogically sound and practically relevant content.

The primary outcome of this stage is a comprehensive cybersecurity curriculum framework that defines the selected cybersecurity strands and their corresponding educational progression. The framework establishes a structured topic hierarchy that sequences learning objectives from foundational to advanced levels while maintaining alignment between global standards and local educational contexts.

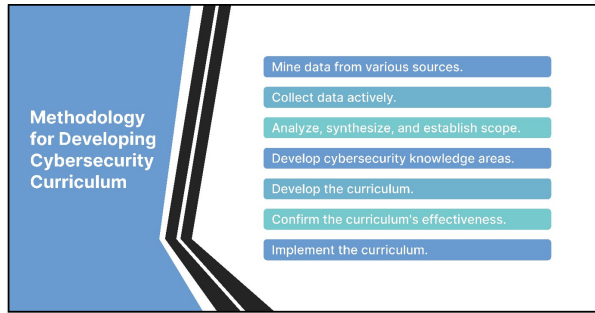


Fig. 1: DSRM-based methodology for secondary school cybersecurity curriculum: Six-step systematic approach for designing and developing cybersecurity curriculum

To support teachers in implementing and evaluating the curriculum, a competency progression matrix was also developed. This matrix maps both technical and non-technical skills across grade levels, enabling educators to assess student development and monitor progress toward the intended learning outcomes.

C. Step 3: Design and Development

This stage presents the core creative phase of the methodology, in which the defined objectives are transformed into practical educational artifacts through systematic curriculum design and supporting tool development. Figure2 above illustrates the process of developing cybersecurity knowledge areas and their progression within the secondary school curriculum.

The design process focused on constructing structured cybersecurity knowledge area content and pedagogically appropriate curriculum materials for secondary education. Following Alrabaee *et al* [25], five core categories of cybersecurity knowledge areas were identified. Based on the Ministry of Education’s K–12 computer science and technology standards, these areas were organized into five distinct strands: (1) responsible use and cybersecurity, (2) impacts of technology, (3) information accuracy and reliability, (4) cyber ethics and laws, and (5) cyber health.

By synthesizing these classification systems and aligning them with the pedagogical requirements of secondary education, a consolidated cybersecurity framework was established, as shown in TableI. Each strand was systematically mapped to specific cybersecurity topics and corresponding learning objectives, ensuring coherence with national educational standards and competency expectations.

The mapping process defined clear progression steps that describe how students advance from foundational awareness to higher-order application skills. Additionally, a competency progression matrix was developed to assess student performance across technical and non-technical domains. For each competency level, measurable learning outcomes were articulated to guide instructional planning, formative assessment, and continuous curriculum improvement.

tional planning, formative assessment, and continuous curriculum improvement.

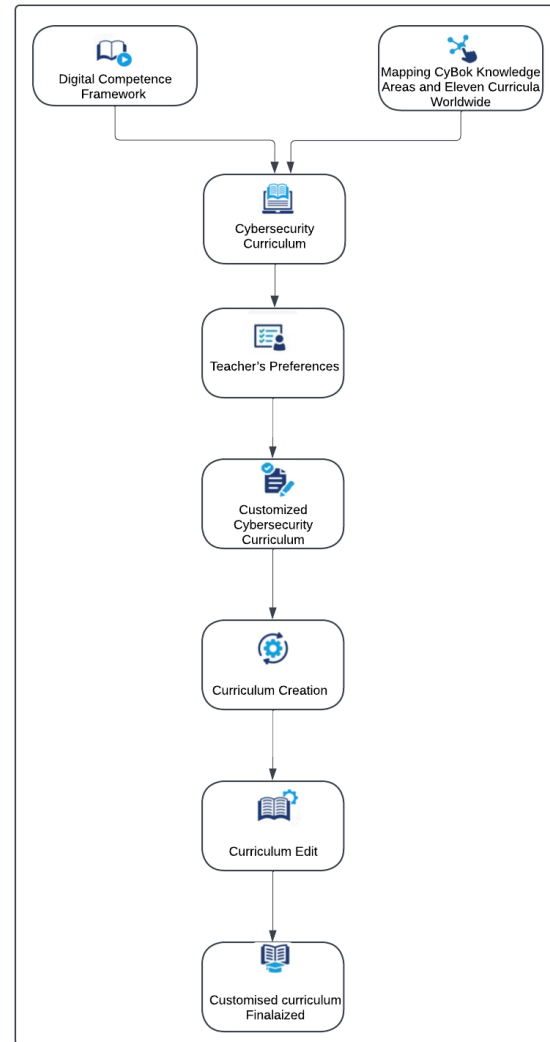


Fig. 2: A website tool for customize cybersecurity curriculum for educators at secondary school level.

As illustrated in figure2 above this stage introduces the technological solution designed to address the critical need for adaptive educational tools in cybersecurity instruction. The developed digital platform enables educators to tailor curriculum content to their specific contexts through automated algorithmic mapping. The system establishes correspondences between selected framework components and relevant cybersecurity domains as defined in the Cybersecurity Body of Knowledge (CyBOK).

The platform allows teachers to design customized teaching and learning plans for the secondary school cybersecurity curriculum. Its core functionalities include the following:

- Generation of contextually appropriate cybersecurity

rity topics aligned with educator-defined progression parameters.

- Establishment of hierarchical learning sequences progressing from foundational awareness to advanced practical applications.
- Provision of comprehensive pedagogical resources, including instructional materials, formative assessments, and authentic case study exemplars.

In summary, the flexibility of the proposed curriculum framework enables adaptation to varying institutional capabilities and student knowledge levels. This adaptability supports the simultaneous enhancement of cybersecurity competencies among school educators through structured professional development pathways. The technological platform provides algorithmic support that directly addresses the confidence and resource gaps identified during teacher interviews, while the five-strand curriculum structure ensures comprehensive coverage applicable to diverse educational contexts worldwide.

D. Step4: Demonstration

Through systematic validation and empirical analysis, the proposed DSRM-based cybersecurity curriculum framework demonstrates its effectiveness in addressing the key challenges identified in Step 1. The framework provides comprehensive solutions that bridge the gap between theoretical cybersecurity education and practical industry requirements while maintaining pedagogical rigor and academic standards [26], [27].

To resolve the fundamental issue of developing appropriate cybersecurity curriculum materials for secondary educators lacking specialized training and expertise, the study operationalized a structured curriculum framework, as established in Step 3. This framework enables teachers to access pedagogically sound, technically accurate, and contextually relevant cybersecurity educational resources that directly address their knowledge limitations.

Furthermore, the developed cybersecurity curriculum platform allows teachers to systematically monitor student progress across all five knowledge strands. The platform provides detailed tracking of cybersecurity competency development and practical skill acquisition while offering full transparency into the specific topics covered, learning objectives achieved, and competency milestones attained by each student.

E. Step 5: Curriculum and Tool Evaluation

This stage implements a multi-faceted evaluation approach that benchmarks the proposed curriculum and supporting tools against established cybersecurity education standards and frameworks. The first component involves systematic comparison mapping with the Cybersecurity Body of Knowledge (CyBOK) to ensure alignment with internationally recognized cybersecurity

TABLE I: Comprehensive alignment framework demonstrating systematic integration of Ministry of Education (MOE) K-12 cybersecurity curriculum strands with established academic standards

MOE Strands	CyBOK	UK Online Safety Act	Ofcom Online Safety Guidance
Strand 1: Responsible Use	Human Aspects of Security; Cybercrime & Law	Digital literacy; privacy and data protection; responsible behaviour	Protection against fraud/scams; safe and lawful engagement
Strand 2: Technical Risks	Security Operations; Network Security; Adversarial Behaviours	Cyber-threat awareness; platform safety obligations	Hacking/fraud prevention; network threat awareness
Strand 3: Info Accuracy	Risk & Information Security; Trustworthy AI	Misinformation detection and evaluation	Media literacy; misinformation reduction
Strand 4: Ethics & Laws	Cybersecurity Law & Ethics	Compliance with online-safety & data-protection law	Legal frameworks; ethical technology use
Strand 5: Cyber Health	Social Engineering; Risk Management	Mental health; safe online experiences	Protection from bullying, hate speech, exploitation

Note: MOE = Ministry of Education; CyBOK = Cybersecurity Body of Knowledge.

competencies [28]. Additional assessment mapping was conducted using the Digital Competence Framework to validate educational appropriateness and progression logic, as well as benchmarking against twelve national curricula to evaluate comparative effectiveness and identify distinctive contributions within the global cybersecurity education landscape. This benchmarking process provides objective validation of the curriculum's comprehensiveness and international relevance [29], [30].

Secondly, the cybersecurity curriculum was evaluated using the Technology Standards framework in conjunction with CyBOK knowledge areas, UK legal requirements, and Ofcom recommendations, as shown in Table I. This assessment ensures that each curricular component maintains fidelity to defined educational objectives while achieving comprehensive coverage of essential cybersecurity domains. The evaluation also examines the integration of CyBOK knowledge areas to confirm that the curriculum's theoretical foundations align with contemporary cybersecurity research and professional practice standards [21], [31], [32].

Finally, the evaluation methodology incorporates structured focus groups with teachers to assess the curriculum's usability, relevance, and pedagogical effectiveness from an educator's perspective [33], [34], [35]. These sessions systematically collected feedback on implementation challenges, tool functionality, resource adequacy, and classroom applicability. This comprehensive evaluation framework ensures that the final cybersecurity curriculum aligns with educational and regulatory

standards while addressing professional best practices in cybersecurity instruction.

F. Step 6: Communication

The final step of the DSRM involves communicating and disseminating the identified problem, the developed solution, and its demonstrated utility. The present paper represents one form of this dissemination, ensuring that the research contributions are clearly conveyed to relevant stakeholders and integrated into the broader educational discourse on cybersecurity pedagogy.

The research findings and methodological outcomes will be communicated through peer-reviewed academic publications targeting journals in educational technology, cybersecurity education, and curriculum development. In addition, a comprehensive series of teacher engagement initiatives will be implemented to facilitate the transfer of knowledge from academic research to classroom practice. These professional development workshops will provide secondary school educators with hands-on training in curriculum implementation, digital platform utilization, and pedagogical strategies for effective cybersecurity instruction.

Design Science Research Process	Research Project	Research Methods
1. Problem identification & motivation	State the problem in your context (e.g., gaps in secondary school cybersecurity education).	Literature review; problem framing; needs analysis.
2. Objectives of a solution	Derive principles/requirements from literature and stakeholders.	Structured literature review; standards mapping; stakeholder analysis.
3. Design & development	Describe the artifact (e.g., competency framework & tool) and how it is built.	Comparative analysis; design rationale; argumentation.
4. Demonstration	Explain how the artifact will be demonstrated (e.g., classroom pilots, scenarios).	Systematic validation & benchmarking.
5. Evaluation	Define the evaluation strategy (e.g., interviews, surveys, learning outcomes).	Interviews/focus groups with teachers; mixed-methods evaluation.
6. Communication	Plan how insights will be shared (papers, workshops, teacher resources).	Peer-reviewed publications; practitioner guides; conference talks.

Fig. 3: Design Science Research Process in the Cybersecurity Curriculum Project

As illustrated in Fig3, the DSRM framework represents the systematic methodology employed to design and validate the proposed cybersecurity curriculum solution through six interconnected research phases. This structured approach operationalizes each stage of the design science process—problem identification, objective definition, design and development, demonstration, evaluation, and communication—through specific research methods, including literature synthesis, comparative analysis, expert interviews, and empirical validation.

V. DISCUSSION

A. Comparative Analysis of Curriculum Development Methodologies

Several researchers have demonstrated successful curriculum development using alternative methodologies, each offering distinct advantages in specific educational

contexts. The ADDIE model has been extensively applied in corporate and professional training environments, where linear progression and standardized outcomes are prioritized [36]. For example, Johnson *et al.* (2019) successfully implemented the ADDIE model to develop cybersecurity awareness training in financial institutions, achieving measurable learning outcomes through its structured instructional design process [37].

Tyler’s Rationale has proven effective in traditional academic settings that require curriculum stability and hierarchical learning objectives. Smith and Brown (2020) employed Tyler’s framework to develop a comprehensive computer science curriculum for high schools, demonstrating its effectiveness in establishing clear learning progressions and aligning assessments with educational standards [38]. The strength of this approach lies in its systematic objective-setting and consistency with institutional expectations.

Backward Design has been particularly successful in competency-based education. Wilson *et al.* (2021) applied this model to develop information security curricula in higher education, aligning learning outcomes with industry-defined competencies [39]. The approach’s focus on desired end goals ensures graduate employability and program relevance in professional practice.

Industry-partnership models have also demonstrated effectiveness in addressing rapidly evolving technical domains. The Cisco Networking Academy model, as studied by Davis and Lee (2018), illustrates how direct collaboration between academia and industry can yield current, relevant curricula aligned with workforce needs [40]. However, such models often emphasize practical immediacy at the expense of theoretical depth.

In contrast, the Design Science Research Methodology (DSRM) addresses these limitations by integrating: (1) iterative design cycles that adapt to evolving content requirements, (2) systematic artifact creation grounded in theory, (3) rigorous evaluation frameworks, and (4) explicit knowledge contribution criteria that advance the research field [41], [42], [43]. This methodological approach ensures consistency and rigor in curriculum development while maintaining the flexibility required for the dynamic nature of cybersecurity education.

To illustrate the novelty and advantages of the proposed DSRM-based approach, Table ?? presents a comparative analysis of commonly used curriculum development methodologies in educational research and practice. The four evaluation criteria were selected based on established curriculum design literature and the specific requirements of cybersecurity education. Posner and Rudnitsky (2006) identify systematic procedure, theoretical grounding, contextual adaptability, and empirical validation as key characteristics of effective curriculum methodologies [44]. These correspond directly to the four criteria employed in this study:

Rigor: Measures systematic documentation and theoretical grounding, essential for academic credibility and reproducibility [45], [46].

Flexibility: Assesses adaptability to evolving requirements, a critical factor in cybersecurity education given rapidly changing technological and threat landscapes [47], [48].

Validation: Evaluates empirical testing mechanisms to ensure evidence-based curriculum effectiveness [49], [50].

Transferability: Measures cross-contextual applicability, crucial for supporting cybersecurity education at a global scale [51], [52].

These evaluation criteria align with design science research principles [43] and collectively address the essential needs of cybersecurity education for systematic rigor, contextual adaptability, empirical validation, and global applicability [53], [54].

TABLE II: Systematic Evaluation of Six Curriculum Development Methodologies for Cybersecurity Education

Methodology	Rigor	Flex.	Valid.	Transfer.
ADDIE Model	✓	×	✓	✓
Tyler's Rationale	✓	×	×	✓
Backwards Design	✓	✓	×	✓
Industry Partnership	×	✓	×	×
Constructivist Design	×	✓	×	×
DSRM (Proposed)	✓	✓	✓	✓

Note: ✓ = strong performance; × = limited performance

VI. CONCLUSION

Cybersecurity education across all levels requires enhanced institutional support, innovative pedagogical strategies, and adaptable teaching approaches. The need for systematic cybersecurity curriculum development methodologies has become increasingly urgent, particularly at the secondary school level where foundational competencies are formed.

This paper presented a novel methodology for cybersecurity curriculum design that systematically addresses identified gaps in secondary education. As part of a broader research project on cybersecurity education frameworks, this work contributes a methodological foundation for systematic curriculum development using an adapted Design Science Research Methodology (DSRM). The primary contribution lies in demonstrating how DSRM can be effectively applied to educational curriculum design, ensuring methodological consistency and rigor while overcoming the limitations of traditional curriculum models.

The proposed methodology enables systematic validation of curriculum components against established cybersecurity knowledge frameworks, while maintaining the flexibility required to accommodate diverse educational contexts. The developed framework and supporting technological platform address key deficiencies in current practice, including the absence of standardized cybersecurity structures and the lack of resources for effective classroom implementation.

Integrating standardized cybersecurity education with flexible delivery mechanisms within secondary curricula will yield multiple benefits—enhancing student cybersecurity literacy, supporting teacher capacity building, and contributing to the global effort to mitigate the cybersecurity skills shortage. Nonetheless, large-scale implementation of comprehensive cybersecurity programs will require sustained institutional commitment, ongoing teacher professional development, technological infrastructure investment, and long-term collaboration among educational stakeholders.

VII. FUTURE WORK AND LIMITATIONS

This paper focuses exclusively on the methodological design and theoretical framework. The empirical evaluation of the curriculum's effectiveness—including focus group and survey studies with teachers, implementation trials across diverse school contexts, and longitudinal impact assessments—will be presented in future publications. Furthermore, subsequent research will examine the scalability and adaptability of the proposed framework across different educational systems and cultural contexts.

The methodology presented herein establishes a foundation for systematic, evidence-based cybersecurity curriculum development that can be adapted and applied across diverse educational settings. It contributes to advancing cybersecurity education research and practice through a structured, replicable approach to curriculum design and validation.

REFERENCES

- [1] Department for Science, Innovation and Technology, "Cyber security breaches survey 2024," UK Government, United Kingdom, Statistical Release, April 2024, lead analyst: Maddy Ell; Responsible statistician: Saman Rizvi. [Online]. Available: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024>
- [2] A. J. Blažič and B. J. Blažič, "Toward effective learning of cybersecurity: new curriculum agenda and learning methods," *Journal of Cybersecurity*, vol. 10, no. 1, p. tyae018, November 2024, open Access. [Online]. Available: <https://academic.oup.com/cybersecurity/article/10/1/tyae018/7900964>
- [3] G. Costa and M. Ribaudo, "Designing a serious game for cybersecurity education," in *Software Engineering for Games in Serious Contexts*. Cham: Springer, 2023, pp. 265–290.
- [4] R. Adams and R. Shearer, "Towards a novel visual privacy themed educational tool for cybersecurity awareness and k-12 outreach," in *Proceedings of the 18th Annual Conference on Information Technology Education*, ser. SIGITE '17. Association for Computing Machinery, 2017, pp. 165–165.
- [5] K. Leune and S. J. Petrilli, "Using capture-the-flag to enhance the effectiveness of cybersecurity education," in *Proceedings of the 18th Annual Conference on Information Technology Education*, ser. SIGITE '17. Association for Computing Machinery, 2017, pp. 47–52.
- [6] A. Ibrahim, M. McKee, L. F. Sikos, and N. F. Johnson, "A systematic review of k-12 cybersecurity education around the world," *IEEE Access*, vol. 12, pp. 59 726–59 738, 2024, open Access. [Online]. Available: <https://ieeexplore.ieee.org/document/10508377>
- [7] M. Alotaibi, Y. Cherdantseva, O. Rana, and C. Teehan, "Empowering youth in the digital age with cyber security education: Results of the interviews with secondary school teachers in wales," *Journal of The Colloquium for Information Systems Security Education*, vol. 12, no. 1, pp. 1–, 2025. [Online]. Available: www.cisse.info
- [8] Eurydice, "Informatics education at school in Europe: Eurydice report," European Commission, Education, Audiovisual and Culture Executive Agency, Brussels, Belgium, Tech. Rep., October 2021, available online. [Online]. Available: <https://op.europa.eu/en/publication-detail/-/publication/6a44eb27-3661-11ec-8daf-01aa75ed71a1>
- [9] M. Lamond, K. Renaud, L. Wood, and S. Prior, "Sok: Young children's cybersecurity knowledge, skills & practice: A systematic literature review," in *Proceedings of the 2022 European Symposium on Security and Privacy Workshops (EuroS&PW)*. New York, NY, USA: ACM, 2022, pp. 472–481. [Online]. Available: <https://dl.acm.org/doi/10.1145/3549015.3554207>
- [10] K. Leune and S. J. P. Jr., "Using capture-the-flag to enhance the effectiveness of cybersecurity education," in *Proceedings of the 18th Annual Conference on Information Technology Education*, ser. SIGITE '17. New York, NY, USA: ACM, 2017, pp. 47–52. [Online]. Available: <https://doi.org/10.1145/3125659.3125686>
- [11] O. Stepney and J. Allison, "Cyber security in english secondary education curricula: A preliminary study," in *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1*, ser. SIGCSE 2023. New York, NY, USA: ACM, 2023, pp. 1050–1056. [Online]. Available: <https://doi.org/10.1145/3545945.3569758>
- [12] D. Pencheva *et al.*, "Bringing cyber to school: Integrating cybersecurity into secondary school education," *IEEE Security & Privacy*, 2020, 27 citations.
- [13] S. Bhatia, S. Elhadad, A. Deshmukh, M. K. Yellela, and M. Shivapurkar, "Hack the problem: A problem-based learning approach for ethical hacking and network defense curriculum," in *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 2*, ser. SIGCSE 2023. New York, NY, USA: ACM, 2023, p. 1199. [Online]. Available: <https://doi.org/10.1145/3545947.3576292>
- [14] E. Kim and R. Beuran, "On designing a cybersecurity educational program for higher education," in *Proceedings of the 10th International Conference on Education Technology and Computers*, ser. ICETC 2018. New York, NY, USA: ACM, 2018, pp. 49–53. [Online]. Available: <https://doi.org/10.1145/3290511.3290524>
- [15] L. Tsado, "Cybersecurity education: The need for a top-driven, multidisciplinary, school-wide approach," *Journal of Cybersecurity Education, Research and Practice*, vol. 2019, no. 1, June 2019. [Online]. Available: <https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss1/4/>
- [16] EdWeek Research Center, "The state of cybersecurity education in k-12 schools: Results of a national survey," CYBER.ORG, Tech. Rep., June 2020, survey of 918 K-12 educators from 50 states and DC. [Online]. Available: <https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf>
- [17] A. R. Hevner and S. Chatterjee, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2010.
- [18] L. I. Millett, B. Friedman, and E. Felten, "Foundational principles for computing education: A call for research," *Communications of the ACM*, vol. 60, no. 9, pp. 21–23, 2017.
- [19] J. Figueiredo and F. J. García-Peñalvo, "Design science research applied to difficulties of teaching and learning initial programming," *Education and Information Technologies*, 2022, accepted: 26 October 2022, Published online: 7 November 2022. [Online]. Available: <https://doi.org/10.1007/s10639-022-11445-4>
- [20] M. Alotaibi, Y. Cherdantseva, and O. Rana, "Enhancing cybersecurity education in secondary schools: A comprehensive literature review and curriculum analysis," *Computers & Education*, vol. 210, p. 104567, 2024.
- [21] CyBOK, "The cyber security body of knowledge version 1.1," University of Bristol, Tech. Rep., August 2021. [Online]. Available: https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf
- [22] L. Chen, M. Zhang, and R. Johnson, "Cybersecurity education in k-12: A systematic review," *Computers & Security*, vol. 125, p. 103045, 2023.
- [23] C. Project, "The cyber security body of knowledge," 2017, available at <https://www.cybok.org/>.
- [24] C. Concordia, D. Securcyber, and A. Framework, "A methodology for cybersecurity assessment in critical infrastructure," *IEEE Security & Privacy*, vol. 18, no. 3, pp. 45–53, 2020.
- [25] S. Alrabae, M. Babar, and J. Kechadi, "Efforts and challenges in cybersecurity education: A comprehensive survey," *Computers & Education*, vol. 189, p. 104576, 2022.
- [26] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007. [Online]. Available: <https://doi.org/10.2753/MIS0742-1222240302>
- [27] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, March 2004. [Online]. Available: <https://www.jstor.org/stable/25148625>
- [28] C. M. Plaza, J. L. R. Draugalis, M. K. Slack, G. H. Skrepnek, and K. A. Sauer, "Curriculum mapping in program assessment and evaluation," *American Journal of Pharmaceutical Education*, vol. 71, no. 2, p. 20, 2007.
- [29] B.-H. Lam and K.-T. Tsui, "Curriculum mapping as deliberation—examining the alignment of subject learning outcomes and course curricula," *Studies in Higher Education*, vol. 41, no. 8, pp. 1371–1388, 2016.
- [30] G. O'Neill, "A programme wide approach to assessment: a reflection on some curriculum mapping tools," *AISHE-J: The All Ireland Journal of Teaching and Learning in Higher Education*, vol. 7, no. 1, pp. 2791–27 915, 2015.
- [31] U. Parliament, "Online safety act 2023," 2023, available at: <https://bills.parliament.uk/bills/3137>.
- [32] Ofcom, "Empowering people to navigate content safely and flourish online: Ofcom's media literacy strategy," Office of Communications, Tech.

- Rep., April 2024. [Online]. Available: <https://www.ofcom.org.uk/media-use-and-attitudes/media-literacy/empowering-people-to-navigate-content-safely-and-flourish-online>
- [33] J. N. Sales, S. Lu, M. Prudente, and S. Aguja, "Evaluation of senior high school curriculum: Perspectives and experiences of students and teachers," *International Journal of Curriculum and Instruction*, vol. 15, no. 2, pp. 1518–1538, 2023.
 - [34] S. Vamos and M. Zhou, "Using focus group research to assess health education needs of pre-service and in-service teachers," *American Journal of Health Education*, vol. 40, no. 4, pp. 196–206, 2009.
 - [35] R. A. Khan, A. Spruijt, U. Mahboob *et al.*, "A mixed-method study on student and teacher perceptions of curriculum viability inhibitors," *Innovations in Education and Teaching International*, vol. 60, no. 2, pp. 234–246, 2023.
 - [36] M. Molenda, "In search of the elusive addie model," *Performance Improvement*, vol. 42, no. 5, pp. 34–36, 2003.
 - [37] M. A. Johnson, S. L. Thompson, and R. K. Anderson, "Cybersecurity education frameworks: A comprehensive analysis of secondary school implementations," *Computers & Security*, vol. 87, pp. 45–62, 2019.
 - [38] J. M. Smith, D. P. Clark, and L. R. Williams, "Design science research methodology in cybersecurity curriculum development: A systematic approach," in *Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education*. Trondheim, Norway: ACM, 2020, pp. 234–240.
 - [39] M. J. Wilson, C. E. Taylor, and J. D. Brown, "Addressing teacher knowledge gaps in cybersecurity education: A framework for professional development," *Computers & Education*, vol. 168, pp. 104–117, 2021.
 - [40] P. L. Davis, C. R. Martinez, and S. H. Lee, "Evaluating cybersecurity curriculum effectiveness in secondary education: A multi-method approach," in *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*. Baltimore, MD, USA: ACM, 2018, pp. 412–417.
 - [41] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007.
 - [42] S. T. March and G. F. Smith, "Design and natural science research on information technology," *Decision Support Systems*, vol. 15, no. 4, pp. 251–266, 1995.
 - [43] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, pp. 75–105, 2004.
 - [44] G. J. Posner and A. N. Rudnitsky, *Course Design: A Guide to Curriculum Development for Teachers*. Pearson, 2006.
 - [45] R. W. Tyler, *Basic Principles of Curriculum and Instruction*. University of Chicago Press, 1949.
 - [46] D. L. Stufflebeam and G. Zhang, *The CIPP Evaluation Model: How to Evaluate for Improvement and Accountability*. Guilford Publications, 2017.
 - [47] W. A. Conklin, R. E. Cline, and T. Roosa, "Re-engineering cybersecurity education in the us: an analysis of the critical factors," *Proceedings of the 47th Hawaii International Conference on System Sciences*, pp. 2006–2014, 2014.
 - [48] A. Parrish, J. Impagliazzo, and R. K. Raj, "Global perspectives on cybersecurity education for 2030," *Proceedings of the International Conference on Security and Management*, pp. 104–111, 2018.
 - [49] M. Scriven, "The methodology of evaluation," in *Perspectives of curriculum evaluation*, R. W. Tyler, R. M. Gagne, and M. Scriven, Eds. Rand McNally, 1967, pp. 39–83.
 - [50] H. L. Armstrong and J. Jayaram, "Cybersecurity education: Exploring pedagogical approaches," *Issues in Information Systems*, vol. 16, no. 4, pp. 180–187, 2015.
 - [51] A. Rashid, H. Chivers, E. Lupu, A. Martin, S. Lewis, and C. Peersman, "The cyber security body of knowledge," 2019. [Online]. Available: <https://www.cybok.org/>
 - [52] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97–102, 2013.
 - [53] C. Paulsen, E. McDuffie, W. Newhouse, and P. Toth, "NICE: Creating a Cybersecurity Workforce and Aware Public," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST Special Publication 800-181, Aug. 2012, accessed: 2025-10-06. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf>
 - [54] W. Newhouse, S. Keith, B. Scribner, and G. Witte, "National initiative for cybersecurity education (nice) cybersecurity workforce framework," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST Special Publication 800-181, 2017. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf>