SELINUS UNIVERSITY
OF SCIENCES AND LITERATURE

The Meta-Analysis of the Professionalisation Frameworks Across Multiple Professions – Successes, Challenges, and Implications for Cybersecurity Design

By Yeow Soon Keong Samson

A DISSERTATION

Presented to the Department of
Strategic Management
program at Selinus University

Faculty of Business and Media
in fulfillment of the requirements
for the degree of Doctor of Philosophy
in Strategic Management

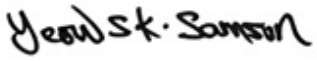
2025

Declaration

I hereby confirm that I am the sole author of this dissertation, and its content is solely the result of my readings, study and research.

I declare that this dissertation entitled **"The Meta-Analysis of the Professionalisation Frameworks Across Multiple Professions – Successes, Challenges, and Implications for Cybersecurity Design**", is entirely my own work and has not been submitted for any other degree or qualification at this or any other institution.

All references and sources of information in this study used have been appropriately acknowledged.



Yeow Soon Keong Samson
UNISE3421IT

Acknowledgements

I am deeply grateful to everyone who has offered their constant encouragement and assistance throughout my doctoral journey.

To my family members and friends, thank you all for your unwavering encouragement and belief in my ability to take on this challenge.

Lastly, my heartfelt appreciation to the secretariat and faculty of the University's Doctoral Programme, with special mention of my advisor, Professor Salvatore Fava. Your guidance and mentorship have been invaluable throughout my learning journey, and I am truly thankful.

Abstract

The aim of this study is to conduct a comprehensive meta-analysis of both the successes and challenges of professionalisation frameworks across a range of established professions. These include medicine, law, engineering, education, and information technology sectors. By systematically reviewing and synthesising the outcomes of these professional frameworks, this study attempts to identify the factors that have contributed to their success. Such factors may include standardisation, ethical guidelines, and continuous professional development, etc. Simultaneously, the study will also examine common challenges and pitfalls that have hindered or obstruct the professionalisation process in certain fields. Such negative factors may include inconsistent certification standards, lack of cohesion between governing bodies, and challenge to adapt to rapidly evolving industry needs. With this meta-analysis, the study will purpose to extract important and valuable insights for designing of a more robust and effective professionalisation framework for the cybersecurity profession. With the unique challenges encountered by cybersecurity professions, such as the dynamic and global nature of cyber threats, fragmented certifications, and the absence of a universally recognised governing body, it is imperatively important and critical to develop a framework that addresses these mentioned complexities and obstacles. The study will focus on designing the proposed framework to ensure that it meets both regional and international demands, while fostering continuous professional learning and ethical accountability within the cybersecurity profession. The ultimate aim is to provide an important pathway for the cybersecurity field to professionalise in a way that enhances one's credibility, trust, and skill development on a global scale.

Keywords: meta-analysis, thematic analysis, mutual recognition agreement, continuous professional development, professionalisation framework, competency framework

Contents

List of Tables

List of Figures

Chapter 1. Introduction

Professionalisation is the process by which a trade or occupation evolves into a recognised and true "profession of the highest integrity and competence" (Nilsson, 2007). This process typically involves the setting of qualification requirements, forming of professional associations to guide the best practices and overseeing the member' conduct and work ethics, and distinguishing qualified and skilled working professionals from unqualified individuals through both academic and professional certifications. This very often also limits the entry into the profession, restricting it to those individuals who meet the specific standards and requirements.

As present cyber threats grow increasingly complex and sophisticated, the need for a skilled and professionalised cybersecurity workforce is more critical and urgent than ever, especially important and true for a market that is shortage of skilled professionals. Many organisations and government agencies worldwide depend on cybersecurity professionals to protect important and sensitive data, critical infrastructure, as well as the application and network systems from attacks by adversaries (Gunther, 2014). However, the lack of a unified, globally recognised framework for professionalising this field has resulted in fragmented qualifications, inconsistent skill sets, and limited professional recognition (Rashid et al., 2018). Unlike established professions such as engineering, law, or healthcare, cybersecurity does not yet benefit from a comprehensive system of certification, ethical standards, and continuous professional development (Evetts, 2013).

In other professional fields, professionalism plays an important role in setting the official standards, to increase credibility and promote public confidence. Professionalism refers to the process by which a profession develops into a recognised profession. Typically, this is done through specialised education & training, certification exams, and the establishment of

ethical codes and regulatory bodies (Evetts, 2013). The process helps to ensure consistency and quality within the profession, and often includes formal career path definitions and standards for continuing professional development. This is due to the global and rapidly changing nature of environment in cybersecurity field. A similar approach is therefore needed to develop the field and meet the growing demand.

As such, the main objective of this study is to conduct a meta-analysis of professional frameworks in established professions. It aims to use their insights to design a professional framework for cyber security. By examining both what works well and what challenges there may be in other areas, this study aims to present a globally applicable framework tailored to the unique challenges of cybersecurity.

1.0 Problem Statement

The cybersecurity profession faces significant challenges in establishing consistent professional standards across regions and industries. Although numerous certifications and qualifications exist in the market, they are often disorganised and fragmented, leading to disparities in skill sets and recognition.

This is a problem as the lack of a unified professionalisation framework limits career mobility and hampers global collaboration. It also hinders the industry's ability to respond effectively to the evolving landscape of cyber threats which requires a resolution to the problem.

Without a clear system for professional development, certification, and ethical guidelines, cybersecurity professionals face barriers in career progression, and employers struggle to ensure they are hiring individuals with the necessary skills and qualifications. To address these issues, this study seeks to draw lessons from other professions that have successfully implemented professionalisation frameworks and use those insights to propose a comprehensive framework for cybersecurity.

1.1 Purpose Statement

This study aims to provide a clear understanding of the critical factors that contribute to successful professionalisation frameworks and how these can be applied to the field of cybersecurity (see Figure 1). The specific objectives of this study are:

1. To conduct a meta-analysis of professionalisation frameworks across professions such as engineering, law, healthcare, and IT, identifying key success factors and common challenge points.
2. To propose a globally recognised, adaptable professionalisation framework for cybersecurity that includes standardised certification, ethical guidelines, continuous professional development, and mechanisms for mutual recognition across regions.

The study will address the following questions:

1. What are the critical success factors and common challenges in the professionalisation frameworks of various fields, and how can these lessons be applied to cybersecurity?
2. How can a standardised, globally recognised professionalisation framework be designed for the cybersecurity profession, considering its regional and industry-specific challenges?
3. What role do mutual recognition agreements and continuous professional development play in ensuring the long-term success of a professionalisation framework for cybersecurity?

1.2 Conceptual Framework

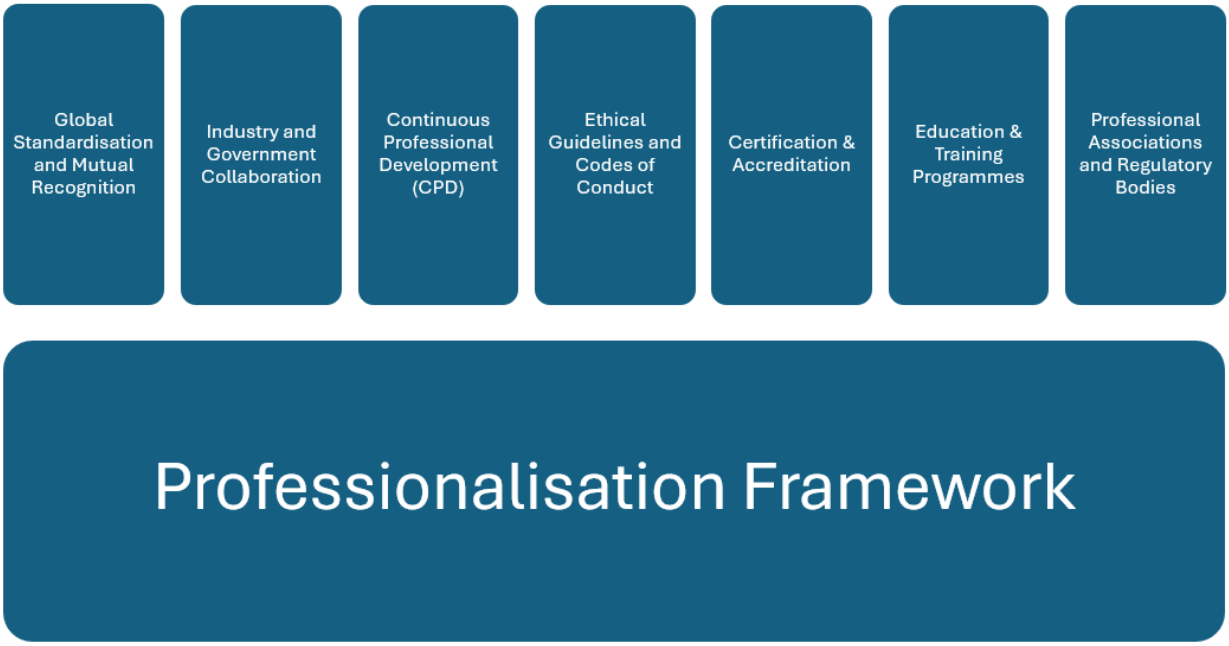
In this study, the goal is to map out the key elements that interact to influence the process of transforming cybersecurity into a recognised and formalised profession. This framework highlights the major components that must work together to ensure a consistent, globally

recognised standard for cybersecurity professionals. The framework (see Figure 1) is flexible, allowing those responsible organisations for adaptation across different regions and industries. Its primary focus is to have the framework that focuses on the interaction of critical factors such as the following:

1. Education and Training Programs
2. Certification and Accreditation
3. Ethical Guidelines and Codes of Conduct
4. Continuous Professional Development (CPD)
5. Industry and Government Collaboration
6. Global Standardisation and Mutual Recognition
7. Professional Associations and Regulatory Bodies

Figure 1

Typical Conceptual Professionalisation Framework



A general conceptual framework for cybersecurity professionalisation typically integrates these seven components, all of which interact to create a structured, standardised approach to recognising and certifying professionals within the cybersecurity field. The framework emphasises the need for a strong educational foundation, reinforced by certification and accreditation processes, underpinned by ethical guidelines, and maintained through continuous professional development.

In this model, industry and government collaboration ensures that the standards remain aligned with real-world needs, while global standardisation and mutual recognition facilitate cross-border cooperation and career mobility. The role of professional associations and regulatory bodies is to oversee the profession, ensuring that it remains credible, ethical, and adaptive to changes.

This framework serves as a general guideline for how the cybersecurity profession can evolve into a fully recognised and standardised field. By focusing on each of the seven key components that have been identified in this study, the framework ensures that cybersecurity professionals are not only technically competent in their job roles but they also subscribe to the code of ethics of the profession and continuously to develop their skills and knowledge in their specialised area that they are responsible for. The study also attempts to identify new opportunities that can be incorporated into the conceptual model taking into consideration of new elements to promote a more holistic approach to professionalisation of cybersecurity.

With the global standardisation and also the mutual recognition of their skills and qualifications, the profession can address the current fragmentation and build a more cohesive and recognised career path for cybersecurity professionals worldwide.

1.3 Significance of the Study

This study is significant because it addresses an important and critical gap in the current approach to formalise the professionalising of cybersecurity professionals. By analysing the successes and challenges of professionalisation frameworks in other fields and the identification of possible new opportunities, this study provides valuable insights that can guide the development of a holistic, comprehensive, globally recognised cybersecurity framework.

A formalised system for professional certification, accountability, ethical guidelines, and continuous professional development will not only raise the standards within the cybersecurity profession but also improve the mobility and recognition of cybersecurity professionals regionally and globally.

The findings from this study will have practical implications for policymakers, educational institutions, certification bodies, and employers in the cybersecurity field. It will help ensure that the cybersecurity profession meets global standards of quality, professionalism, and trust.

1.4 Summary

The scope of this study is focused on analysing the professionalisation frameworks across multiple professions that have been identified. These included the engineering, law, healthcare, and IT fields. The study will primarily rely on a meta-analysis of the existing literature and case studies, in order to identify those important key factors that contribute to the success or challenge of professionalisation efforts. The findings will attempt to identify the critical success factors to follow, challenges to avoid and new opportunities that can be incorporated.

Subsequently these factors will be used to develop a universally accepted framework, specifically designed for the cybersecurity profession both globally and regionally. This will

take into account those global and regional variations, as well as mutual recognition of qualification and experience requirements. This study will not just delve into specific technical skills within cybersecurity but will instead focus on the broader professionalisation processes, including certification requirement, ethical standards, and continuous professional development.

Chapter 2. Literature Review

2.0 Introduction

The literature review aims to provide a comprehensive analysis of the existing professionalisation frameworks across multiple professions, identifying the critical success factors. This chapter will establish the theoretical foundation for the meta-analysis, exploring key concepts such as professionalisation, competency-based frameworks, ethical standards, and continuous professional development. It will also examine the challenges faced by emerging professions, including cybersecurity, that lack a cohesive and universally accepted professionalisation model.

2.1 Understanding Professionalisation: Key Concepts and Definitions

Professionalisation refers to the process by which an occupation develops into a recognised profession. This process includes formal education, certification, accreditation, ethical guidelines, and ongoing professional development. In established professions such as medicine, law, and engineering, the journey toward professionalisation has been gradual but highly structured, with a clear focus on setting standards for practice and upholding ethical integrity. In contrast, emerging fields such as cybersecurity are still in the process of defining and formalising their standards.

Scholars like Freidson (2001) argue that professionalisation is not just about meeting technical competencies, but also about fostering a culture of continuous improvement, ethical practice, and social responsibility. This section will discuss how these components play out across various professions and what lessons can be drawn from them.

2.2 Historical Development of Professionalisation Frameworks

A review of the historical evolution of professionalisation frameworks reveals that the path to becoming a recognised profession often involves overcoming a range of challenges,

including fragmented education systems, varying regional standards, and resistance to formal oversight. For instance, the medical profession's journey toward professionalisation was marked by the establishment of standardised medical education, rigorous licensing examinations, and the enforcement of ethical guidelines like the Hippocratic Oath (Hippocratic Oath, 2018). The legal profession similarly evolved through the development of bar associations and the requirement for lawyers to pass rigorous exams before being licensed to practice.

This section will trace the development of professionalisation frameworks in key professions, highlighting milestones such as the creation of governing bodies, the introduction of licensing and certification exams, and the establishment of ethical codes. The section will also explore how these frameworks have been adapted and refined over time in response to technological advancements, societal changes, and globalisation.

2.3 Professionalisation in Various Sectors: A Comparative Overview

This section will provide a comparative analysis of professionalisation frameworks in five key professions: engineering, law, healthcare, information technology and cybersecurity. Each of these professions has developed unique frameworks tailored to their specific needs and challenges, offering valuable insights for the development of a cybersecurity professionalisation framework.

2.3.1 Engineering

Professionalisation in engineering has been achieved largely through the establishment of global standards and mutual recognition agreements. The Washington Accord, signed in 1989, is an international agreement that recognises the substantial equivalency of engineering education programmes accredited by its signatories. This agreement defines the graduates' attributes (see Appendix A) and also allows engineering professionals to work across borders

without needing to be re-certified, offering a key insight into the role of mutual recognition in professionalisation (Washington Accord, 2021).

In addition to global recognition, engineering professional bodies, such as the Institution of Civil Engineers (ICE) and the Institution of Mechanical Engineers (IMechE) in the UK, play a critical role in enforcing standards, offering certifications like Chartered Engineer (CEng), and providing ongoing professional development. These organisations help maintain the profession's credibility by ensuring adherence to ethical guidelines and continuous learning.

2.3.2 Law

The legal profession offers another model for professionalisation, characterised by a strong focus on ethical standards (see Appendix B) and rigorous certification processes (SRA, 2018b). Legal professional bodies, such as the Law Society of England and Wales and the Bar Council, are responsible for setting educational requirements, conducting bar examinations, and maintaining professional conduct through ethical codes. Professionalisation in law is reinforced by mandatory continuous professional development (CPD) programmes to ensure that legal practitioners stay current with evolving laws and practices (Davies, 2005).

However, the legal profession has faced challenges related to global standardisation. Unlike engineering, the legal field is subject to significant jurisdictional differences, making it difficult to implement mutual recognition agreements. This has limited the global mobility of legal professionals, a challenge that cybersecurity must consider when designing its own professionalisation framework.

2.3.3 Healthcare

Healthcare, particularly the medical profession, is another well-established field with a robust professionalisation framework. The General Medical Council (GMC) in the UK oversees the licensing, revalidation, and ethical standards for medical practitioners. Doctors must

undergo a standardised process of education, certification, and continuous professional development to maintain their professional status (see Appendix C). The ethical standards in healthcare, often seen as one of the highest in any profession, are critical in maintaining public trust (Steven et al., 2017).

One of the key success factors in the healthcare profession is the integration of CPD and revalidation, ensuring that professionals stay up-to-date with the latest medical advancements. This could serve as a model for the cybersecurity field, where technology evolves rapidly, necessitating continuous learning.

2.3.4 Information Technology (IT)

Information technology (IT) offers valuable insights into the professionalisation challenges faced by rapidly evolving fields. Unlike established professions, IT has struggled with fragmentation due to the sheer number of certifications and a lack of cohesive standards.

Entry-level certifications such as CompTIA's A+ and Network+, Project Management Institute's Project Management Professional (PMP), are widely recognised, but they are not universally standardised, leading to discrepancies in skill levels and recognition across regions (Schlag, 2004).

The IT field also highlights the difficulties of achieving global standardisation and mutual recognition. The absence of a global regulatory body, similar to those in engineering or healthcare, has resulted in a lack of unified ethical standards and professional guidelines. This has created a gap in the professionalisation of IT, a challenge that cybersecurity must address as it seeks to formalise its own profession.

2.3.5 Cybersecurity

The professionalisation of cybersecurity is still in its early stages. There are numerous certifications, such as Certified Information Systems Security Professional (CISSP), Certified

Ethical Hacker (CEH), and Certified Information Security Manager (CISM), but there is no single, universally accepted standard for what constitutes a qualified cybersecurity professional (Ozkaya, 2019). The fragmented certification landscape makes it difficult to ensure consistent skill levels and hampers the mobility of professionals across borders.

Cybersecurity also lacks a centralised body responsible for regulating the profession or enforcing ethical guidelines globally. While organisations such as International Information System Security Certification Consortium (ISC2) and Information Systems Audit and Control Association (ISACA), SysAdmin Audit Network and Security (SANS) provide certifications and ethical codes, these do not hold the same weight as the regulatory bodies in healthcare or law. Moreover, the rapidly evolving nature of cyber threats makes continuous professional development critical, yet many certifications do not require ongoing education or revalidation.

2.4 Success Factors in Professionalisation Frameworks

Several key success factors can be identified across various professionalisation frameworks in established fields such as engineering, law, healthcare, and IT. These factors offer valuable lessons for the professionalisation of cybersecurity and are crucial for creating a globally recognised and trusted profession.

2.4.1 Education and Training Programmes

A consistent education pathway is critical for ensuring that professionals in any field meet a minimum standard of competence. In professions like engineering, global agreements such as the Washington Accord have played a significant role in standardising education across various countries. This has made it easier for professionals to have their qualifications recognised internationally, ensuring that they meet consistent educational standards no matter where they are trained (Washington Accord, 2021). The establishment of such global

frameworks increases the credibility of the profession by ensuring that professionals have received a quality education aligned with global standards.

In healthcare, clear education pathways are similarly crucial. Regulatory bodies, such as the General Medical Council (GMC) in the UK, oversee these education programmes to ensure that professionals possess the necessary knowledge and skills before entering practice. This structured approach to education helps to maintain the competence of healthcare professionals, ensuring that they are properly prepared for the demands of their profession.

2.4.2 Certification and Accreditation

Certification and accreditation processes are essential in professionalisation as they validate that individuals have met the necessary standards to practice. In engineering, international frameworks like the Washington Accord not only standardise education but also facilitate the recognition of qualifications across borders, thus enabling engineers to work in different countries with relative ease (Patil & Codner, 2007; Washington Accord, 2021). This standardised approach ensures that accredited professionals meet the same level of competence globally, thereby enhancing the profession's credibility and trustworthiness.

In the healthcare sector, certification and accreditation serve as gatekeepers to ensure that professionals are qualified to provide safe and effective services. Regulatory bodies such as the GMC set rigorous standards for medical professionals to ensure patient safety and public trust in the healthcare system. Standardisation of these certification processes helps maintain high-quality healthcare services, as only those who have met stringent certification requirements are allowed to practice (Steven et al., 2017). This ensures consistent care and protects the public by holding professionals accountable to uniform standards.

2.4.3 Ethical Guidelines and Regulatory Bodies

Strong ethical standards and the presence of regulatory bodies are key to maintaining public trust in a profession. The legal profession, for example, maintains high ethical standards through organisations like the Law Society of England and Wales, which sets ethical guidelines and ensures that members adhere to them through strict oversight (Steven et al., 2017). These standards protect the public and ensure that legal practitioners uphold integrity and professionalism.

Similarly, the GMC enforces ethical codes in the medical field, holding practitioners accountable for their actions and maintaining high professional standards. The emphasis on ethics in both law and healthcare ensures that professionals not only meet technical qualifications but also act in the public's best interest.

2.4.4 Continuous Professional Development (CPD)

Professions like medicine and law place significant emphasis on continuous professional development (CPD), ensuring that professionals remain competent and current in their fields. In healthcare, doctors must regularly update their knowledge through CPD, which is required for revalidation by the General Medical Council (GMC) (Steven et al., 2017). This ensures that they remain skilled in the latest medical practices and technologies.

In a rapidly evolving field like cybersecurity, continuous learning is essential due to the constant development of new threats and technologies. Incorporating mandatory CPD into a professionalisation framework for cybersecurity will ensure that professionals stay up to date with the latest security practices and tools.

2.4.5 Industry and Government Collaboration

A significant success factor in the professionalisation of any field is the collaboration between industry and government. This partnership helps align educational standards, regulatory frameworks, and professional requirements with the evolving needs of the workforce

and the broader economy. When industries and governments work together, they can create policies that ensure the workforce is equipped with the necessary skills and competencies, fostering a dynamic and adaptable professional environment.

Such collaboration also enables the development of relevant certifications and training programmes, ensuring that professionals are both well-trained and accountable to consistent standards. Furthermore, industry input allows for a more responsive regulatory environment that can adapt to technological advancements and global trends, while government oversight ensures the public interest is protected. This synergy not only enhances the credibility and legitimacy of professions but also strengthens their capacity to contribute to national and global economic growth (Brockmann et al., 2008).

2.4.6 Global Standardisation and Mutual Recognition

The success of engineering as a globally recognised profession is due in large part to agreements like the Washington Accord, which enables the mutual recognition of engineering qualifications between member countries (Washington Accord, 2021). Such agreements allow professionals to work across borders without needing additional certification, promoting mobility and collaboration.

Mutual recognition agreements are essential for any profession that seeks to operate globally. By ensuring that certifications are accepted internationally, cybersecurity professionals could move freely between regions, improving global security efforts and addressing the current fragmentation in the profession.

2.4.7 Professional Associations and Regulatory Bodies

A key success factor in the professionalisation of any field is the establishment of strong professional associations and regulatory bodies. For example, in Singapore context, the professional bodies such as both the Association of Information Security Professionals (AiSP)

and Singapore Computer Society (SCS), working closely with the Cyber Security Agency (CSA) of Singapore. These organisations play a pivotal role in setting and maintaining standards of practice, ensuring that professionals meet ethical and competency requirements, and advocating for the interests of the profession. Professional associations provide a platform for networking, continuing education, and the development of best practices, all of which contribute to the professional growth and recognition of members. Regulatory bodies, on the other hand, enforce legal and ethical standards through certification, licensing, and disciplinary procedures.

By creating a structured framework for accountability and skill development, these bodies help ensure that professionals maintain high levels of competence, integrity, and public trust. Moreover, regulatory bodies often collaborate with educational institutions to ensure that training and certification align with industry needs, further strengthening the professionalisation process. Together, professional associations and regulatory bodies serve as the backbone of a profession's legitimacy and continuous improvement, driving both individual career success and the overall advancement of the field (Greenwood et al., 2002).

2.5 Challenges in Professionalisation Frameworks

While many professions have successfully implemented professionalisation frameworks, several challenges remain. These challenges are particularly pronounced in newer or rapidly evolving fields like IT and cybersecurity, where fragmentation, resistance to standardisation, and the pace of technological change complicate the professionalisation process.

2.5.1 Fragmentation in Certification Systems

One of the most significant challenges in professionalisation is the fragmentation of certification systems, particularly in fields like IT and cybersecurity. These fields are

characterised by a multitude of certifications, each with varying levels of recognition and credibility. For instance, in IT, certifications like CompTIA A+ & Network+, CCNA, and PMP, validate different skill sets, but no single body ensures consistency across these certifications (Schlag, 2004).

In cybersecurity, certifications such as CISSP, CEH, CISM, SANS/GIAC Penetration Tester Certification (GPEN), Offensive Security Certified Professional (OSCP), CREST Certification, Foundstone Ultimate Hacking Certification, Certified Penetration Testing Consultant (CTPC), and Certified Penetration Testing Engineer (CPTE), are widely recognised but are not aligned, resulting in inconsistencies in skills and knowledge across the profession. This fragmentation makes it difficult for employers to assess qualifications consistently and hinders the development of a cohesive, universally recognised professionalisation framework (Tretko et al., 2020).

2.5.2 Resistance to Standardisation

Resistance to standardisation is another challenge that many professions face. The legal profession, for example, has historically been resistant to standardisation due to jurisdictional differences in laws and practices. Attempts to create global standards often face pushback because legal professionals are bound by the specific regulations of their country, making it difficult to implement a universally accepted framework (Davies, 2005).

This resistance can also be observed in cybersecurity, where different countries have their own regulatory frameworks for data protection and security practices. Achieving global standardisation in cybersecurity may face challenges similar to those in the legal profession, as different countries have varying security protocols and laws governing cyber practices.

2.5.3 Lack of Ethical Oversight

Professions like medicine and law benefit from strong ethical oversight, enforced by regulatory bodies that hold professionals accountable for their actions. In contrast, fields like IT and cybersecurity have struggled to establish similarly strong ethical frameworks. While organisations like ISC2 and ISACA provide ethical codes as part of their certification processes, these are not universally enforced, and there is no global body responsible for overseeing the ethical conduct of cybersecurity professionals (Manjikian, 2023).

Without strong ethical oversight, the cybersecurity profession risks losing credibility, as unethical practices can go unchecked. Ethical guidelines must be a core component of any professionalisation framework, with a governing body in place to enforce standards and ensure accountability.

2.5.4 Occupational Closure and Exclusion

Professionalisation can sometimes fail by becoming overly exclusive, creating barriers for qualified individuals to enter the profession. This is referred to as occupational closure, where the profession is "closed off" to outsiders or those who cannot afford the necessary education and certification processes (Evetts, 2013).

In fields like law and medicine, the high cost of education and long certification processes can deter talented individuals from entering the profession. This could become a risk for cybersecurity if the professionalisation framework focuses too heavily on high-cost certifications without providing alternative pathways for skilled professionals to gain recognition.

2.5.5 Rapid Technological Change

One of the unique challenges faced by professions like IT and cybersecurity is the rapid pace of technological change, which makes it difficult to keep professional standards and certifications up to date. In these fields, new tools, threats, and technologies emerge constantly,

meaning that certifications that were relevant a few years ago may no longer cover current practices or technologies.

To address this challenge, any professionalisation framework for cybersecurity must include CPD and re-certification processes to ensure that professionals remain competent in a constantly evolving landscape (Moskowitz, 2022).

2.5.6 Inadequate Global Standardisation

The lack of global standardisation is a recurring challenge in the professionalisation of emerging fields. Professions like engineering have successfully implemented global standardisation through agreements like the Washington Accord, but fields such as IT and cybersecurity have struggled to achieve similar recognition. Without global standardisation, cybersecurity professionals may find that their qualifications are not recognised across borders, limiting their mobility and hindering global collaboration (Washington Accord, 2021).

Achieving global standardisation in cybersecurity is essential for creating a cohesive profession. This will require collaboration between governments, industry leaders, and certification bodies to ensure that qualifications are recognised internationally, promoting a more unified global cybersecurity workforce.

2.5.7 Diversity of Cybersecurity Body-of Knowledge

The diversity of Body Of Knowledge (BoKs) in cybersecurity represents both a strength and a significant challenge for the field. As the global cybersecurity landscape evolves, different countries and regions have developed their own BoKs to address the unique needs of their industries, government agencies, and educational institutions. While this diversity fosters tailored approaches to cybersecurity, it also presents challenges in achieving global standardisation, interoperability, and consistent skill development.

One key challenge is the lack of alignment between different BoKs, which can lead to fragmentation in cybersecurity education, certification, and workforce development. Professionals trained in one region may lack the necessary competencies or certifications recognised in another, hindering global mobility and collaboration. For instance, the National Initiative for Cybersecurity Framework (NICE) in the United States, developed by National Institute of Standards and Technology (NIST), may emphasise different competencies than the Cybersecuirty Body of Knowledge (CyBOK) in the United Kingdom or Singapore's Information Security Body of Knowledge IS-BOK 2.0 developed by the Association of Information Security Professionals (AiSP), creating disparities in expertise across borders.

Additionally, inconsistencies in the focus of different BoKs—with some prioritising technical knowledge while others emphasise legal, policy, or ethical issues—can result in cybersecurity professionals being unequally equipped to handle the full spectrum of cybersecurity challenges. This makes it difficult for organisations operating in a globalised world to assess and ensure the comprehensive preparedness of their cybersecurity teams.

Lastly, the challenge of continuous updates and relevance exacerbates these issues, as the rapid pace of technological change demands that each BoK evolves constantly. However, not all regions may be equally agile in updating their frameworks, leading to knowledge gaps in certain areas of cybersecurity, such as emerging threats like Artificial Intelligence (AI)-driven attacks or quantum computing vulnerabilities.

To overcome these challenges, greater efforts are needed to foster collaboration and alignment between the various body of knowledge (see Table 1) to ensure a more cohesive and unified global cybersecurity workforce capable of addressing increasingly complex cyber threats.

Table 1

List of Cybersecurity Body of Knowledge (BOK)

Country/Region	Body of Knowledge	Description
1. United Kingdom	Cybersecurity Body of Knowledge (CyBOK). (2019).	A comprehensive guide covering 19 knowledge areas across domains such as risk management, cryptography, and governance.
2. United States	NICE Cybersecurity Workforce Framework. (2020).	A structured approach to identifying knowledge, skills, and competencies needed for cybersecurity roles.
3. European Union	European Union Agency for Cybersecurity (ENISA). (2022).	Defines cybersecurity knowledge areas to align skills across EU member states.
4. Israel	Israel - National Cyber Security Framework. (2020).	Provides guidelines and best practices technical and policy domains.
5. Singapore	Association of Information Security Professionals (AiSP)'s IS-BOK 2.0: Information Security Body of Knowledge. (2022).	Outlines essential cybersecurity knowledge areas for education and workforce development.

2.5.8 Lack of Unified Cybersecurity Skill Framework

The lack of a unified cybersecurity skill framework across different countries creates significant challenges in building a strong, global cybersecurity workforce. As cybersecurity threats grow, having varied frameworks (see Table 2) in place—like the NICE Framework in the U.S., the UK Cyber Security Council's Career Pathways, or Singapore's Cybersecurity Skills Framework—leads to inconsistent skills and training for professionals around the world.

This inconsistency makes it hard for organisations, especially global ones, to ensure their cybersecurity teams are equally skilled. Certifications and skills recognised in one country

may not be accepted in another, limiting professionals' job mobility and leading to mismatches in employer expectations and employee qualifications.

The rapid pace of new cyber threats also adds pressure, as each region's framework may not update quickly enough to keep professionals prepared for emerging risks. To solve these issues, there needs to be more collaboration and standardisation between frameworks worldwide. This would help create a more capable and unified cybersecurity workforce to handle global threats.

Table 2

List of Cybersecurity Skill Frameworks

Country/Region	Skill Framework	Description
1. United States	NICE Cybersecurity Workforce Framework (NIST). (2020)	Developed by NIST, it provides a comprehensive guide to cybersecurity roles, skills, and competencies across seven categories.
2. Singapore	SkillsFuture Singapore: Cybersecurity Skills Framework. (2019)	Part of Singapore's SkillsFuture initiative, it outlines career paths, job roles, skills, and competencies for the cybersecurity workforce.
3. European Union	European Cybersecurity Skills Framework (ECSF). (2022)	Published by ENISA, the ECSF defines 12 cybersecurity profiles and associated skills and competencies.
4. Japan	IPA: Cybersecurity Workforce Framework (Japan). (2019)	Developed by the Information-Technology Promotion Agency (IPA), it defines job roles, skills, and career paths in cybersecurity.
5. United Kingdom	UK Cyber Security Council – Career Pathways Framework. (2021)	The UK framework provides structured career pathways and competencies for various roles in cybersecurity.
6. Australia	Australian Cyber Security Skills Framework (ACSF). (2018)	Outlines skills and career development paths for cybersecurity professionals, aligning with national industry and government needs.

Country/Region	Skill Framework	Description
7. Canada	Canadian Cybersecurity Competency Framework. (2020)	Defines the skills and competencies required for cybersecurity roles in the public and private sectors.

The comparison of professionalisation frameworks (see Table 3) across various professions reveals significant differences and similarities in how each field has approached the process of establishing standards, certifications, ethical guidelines, and CPD. These frameworks play a crucial role in maintaining the credibility, trust, and effectiveness of professionals within their respective fields. By examining the frameworks in medicine, law, engineering, education, and information technology, we can gain insights into the elements that contribute to successful professionalisation, as well as the challenges that certain professions continue to face.

Table 3

Comparison of Professionalisation Framework Across Professions

Profession	Professional Body	Certification	Ethical Guidelines	Continuous Professional Development (CPD)
1. Medicine	American Medical Association (AMA), General Medical Council (GMC)	Board Certification, Medical Licensing Exams	Hippocratic Oath, Medical Code of Ethics	Mandatory, Required for Re-licensure
2. Law	American Bar Association (ABA), Law Society (UK)	Bar Examination, Legal Licensing	Legal Code of Ethics, Client Confidentiality	Mandatory, CPD Units for Renewal
3. Engineering	Institution of Engineering and	Professional Engineer (PE),	Code of Ethics for Engineers	Mandatory for Chartered Status, Ongoing CPD

Profession	Professional Body	Certification	Ethical Guidelines	Continuous Professional Development (CPD)
	Technology (IET), IEEE	Chartered Engineer (CEng)		
4. Education	Council for the Accreditation of Educator Preparation (CAEP)	Teaching Certification, Professional Educator License	Teacher Code of Ethics	Encouraged, Required for Certain Certifications
5. Information Technology	International Information System Security Certification Consortium (ISC2), CompTIA	Certified Information Systems Security Professional (CISSP), CompTIA Security+	ISC2 Code of Ethics, IT Security Guidelines	Mandatory for Certification Maintenance

In the field of medicine, the professionalisation framework is highly structured and rigorous, overseen by prominent bodies such as the American Medical Association (AMA) and the General Medical Council (GMC). These organisations enforce strict certification processes, including board certification and medical licensing exams, which are essential for practice. Additionally, the medical profession upholds strong ethical standards through the Hippocratic Oath and a comprehensive medical code of ethics. Continuous professional development is mandatory, with physicians required to participate in ongoing education to maintain their licensure. This well-established framework ensures that medical professionals are consistently trained, ethically grounded, and competent in their practice.

Similarly, the legal profession has developed a robust framework that emphasises ethical practice, competency, and continuous learning. Governed by bodies such as the American Bar Association (ABA) and the Law Society in the UK, the legal profession requires practitioners to pass rigorous bar examinations and adhere to strict ethical codes, including client confidentiality. Continuous professional development is also mandatory, with legal

professionals required to complete CPD units for license renewal. This framework has helped the legal profession maintain high standards of practice and adapt to evolving legal challenges.

Engineering, another well-established profession, has a framework that focuses on standardisation and global recognition. Organisations like the Institution of Engineering and Technology (IET) and IEEE play a central role in accrediting engineers through certifications such as Professional Engineer (PE) and Chartered Engineer (CEng). The engineering profession is also governed by a code of ethics that emphasises safety, responsibility, and integrity. Continuous professional development is mandatory for engineers seeking chartered status, ensuring that they remain updated on technological advancements and industry standards. This emphasis on standardisation and ongoing learning has helped engineering maintain its status as a globally respected profession.

In contrast, the education profession has faced challenges in achieving a consistent professionalisation framework. While there are bodies such as the Council for the Accreditation of Educator Preparation (CAEP) that oversee teacher certification and professional educator licenses, the lack of standardisation across regions has led to varied certification requirements and inconsistent teaching quality. Although ethical guidelines exist in the form of a teacher code of ethics, the enforcement and adoption of these standards vary widely. Continuous professional development is encouraged but is not uniformly mandated across all regions, contributing to disparities in professional recognition and teaching practices.

Information technology (IT) presents a unique case where professionalisation has been fragmented due to the rapid evolution of the field and the proliferation of vendor-specific certifications. Early certifications offered by companies like Microsoft and Cisco led to a lack of cohesive global standards, creating confusion in the market. However, organisations like the ISC2 and CompTIA have since emerged, offering more standardised certifications such as

CISSP and CompTIA Security+. The IT profession has increasingly recognised the importance of continuous professional development, with mandatory CPD requirements for certification maintenance. Despite these efforts, the IT sector continues to grapple with the challenge of achieving a universally accepted professionalisation framework.

The comparison of professionalisation frameworks across these professions highlights the importance of standardisation, ethical guidelines, and continuous professional development in maintaining the integrity and effectiveness of professionals. While fields like medicine, law, and engineering have successfully established cohesive frameworks, education and IT face ongoing challenges in achieving consistent professionalisation. These insights can be invaluable in informing the development of a robust and effective professionalisation framework for cybersecurity, a field that currently lacks a universally recognised standard but is increasingly vital to global security.

2.6 Summary

This chapter explored the professionalisation frameworks in various established professions such as engineering, law, healthcare, and IT, and examined their relevance to the emerging field of cybersecurity. Key success factors identified across these professions include standardised education and certification, the establishment of ethical guidelines, and the incorporation of continuous professional development (CPD). Professions like engineering have benefitted from global standardisation and mutual recognition agreements, while fields such as law and healthcare have maintained public trust through strict ethical oversight and regulatory bodies.

However, the review also highlighted significant challenges, particularly in rapidly evolving fields like IT and cybersecurity. These challenges include fragmented certification systems, inconsistent global standards, and the difficulty of keeping up with technological

advancements. The current state of cybersecurity professionalisation reflects these issues, with a wide array of certifications but no universally accepted standard or centralised regulatory body.

The insights gained from this review will serve as the foundation for proposing a more cohesive and standardised professionalisation framework for cybersecurity. By addressing the fragmentation and integrating global standardisation, ethical oversight, and CPD, the cybersecurity profession can advance towards becoming a fully recognised and trusted field globally.

Chapter 3. Methodology

3.0 Introduction

This chapter outlines the study methodology employed in this study, focusing on the use of meta-analysis as the primary study technique. Meta-analysis is a quantitative and systematic approach to synthesising findings from multiple studies to identify patterns, strengths, and gaps in existing study. This method is particularly well-suited for this study, which aims to analyse professionalisation frameworks across various professions and apply the findings to the development of a comprehensive framework for cybersecurity.

The methodology section will cover the study design, data collection procedures, inclusion and exclusion criteria, and the data analysis process, as well as how the findings from the meta-analysis will inform the design of the cybersecurity professionalisation framework.

3.1 Study Design

The study follows a meta-analytic design, which involves collecting, analysing, and synthesising data from multiple studies on professionalisation frameworks across different fields, including engineering, law, healthcare, and information technology (IT). The goal is to aggregate findings from various sources to identify the success factors and challenges that have influenced the professionalisation process in these fields. These insights will then be applied to propose a more structured and standardised professionalisation framework for cybersecurity.

The use of meta-analysis allows for a comprehensive examination of the existing literature, ensuring that the findings are robust and represent a broad spectrum of professionalisation efforts.

3.2 Meta-Analysis Approach

Meta-analysis provides a structured method for combining results from multiple empirical studies. It is a statistical technique used to systematically review, synthesise, and

summarise findings from multiple studies, allowing researchers to derive conclusions based on a collective body of evidence (Field & Gillett, 2010). It is commonly used in various fields, including medicine, education, and the social sciences, and increasingly in cybersecurity and professionalisation studies, as it offers a way to identify patterns, measure overall effects, and address inconsistencies in findings across different studies.

For each study, the following fields will be used to work out the necessary information needed to perform the analysis (refer to Table 12), namely:

- Pooled Standard Deviation (SD_{pooled})
- Cohen's d
- Standard Error (SE)
- Variance
- Weight

3.2.1 Pooled Standard Deviation (SD_{pooled})

The pooled standard deviation is a measure used to estimate the common standard deviation for two or more groups when conducting a comparison, such as in a t-test (Pearson, n.d.) or when calculating effect sizes like Cohen's d (Cohen, 1988, 1992; Ellis, 2010). It combines the standard deviations of the individual groups into a single, weighted average that accounts for the different sample sizes of the groups.

3.2.1.1 Formula.

$$\boldsymbol{S\,D}_{\textbf{pooled}} = \sqrt{\frac{(\boldsymbol{n1}-\boldsymbol{1})\boldsymbol{x}\ \boldsymbol{SD1^2} + (\boldsymbol{n2}-\boldsymbol{1})\ \boldsymbol{x}\ \boldsymbol{SD2^2}}{\boldsymbol{n1}+\boldsymbol{n2}-\boldsymbol{2}}} \qquad (1)$$

3.2.1.2 Explanation:

- ***SD1*** and ***SD2***: These are the standard deviations of the two groups.

- ***n1*** and ***n2***: These are the sample sizes of the two groups.
- ***n1 - 1*** and ***n2 - 1***: These are the degrees of freedom for each group. They are used to weight the standard deviations of each group, giving more influence to the group with a larger sample size.

3.2.1.3 Purpose:

The pooled standard deviation is used to:

Combine Variability: It provides a single estimate of variability that assumes the groups have the same variance (homogeneity of variance). This assumption is crucial in many statistical tests.

Calculate Effect Sizes: When comparing the means of two groups, the pooled standard deviation is used in the denominator of Cohen's d to standardise the mean difference.

3.2.1.4 When to Use:

Equal Variances Assumed*:* It's used when the assumption of equal variances across the groups is reasonable. If the variances are very different, you might need to use other methods (like Welch's t-test) that do not assume equal variances.

3.2.2 Cohen's d

Cohen's d is a measure of effect size that quantifies the difference between two group means in terms of standard deviations. It provides a standardised way to assess how much the groups differ from each other.

3.2.2.1 Formula.

$$\boldsymbol{d = \frac{M1 - M2}{S\,D_{\text{pooled}}}} \qquad (2)$$

3.2.2.2 Explanation:

Numerator (Difference in Means): The difference between the means of the two groups (*M1 – M2*) shows the absolute difference in the outcomes being measured.

Denominator (Pooled Standard Deviation): The pooled standard deviation (SD_{pooled}) normalises this difference by accounting for the variability within the groups. This makes the effect size independent of the units of measurement.

3.2.2.3 Purpose:

Cohen's d serves several important purposes in statistical analysis:

Standardisation: By expressing the difference between groups in terms of standard deviations, Cohen's d allows for the comparison of effect sizes across different studies, even when the studies use different scales or units of measurement.

Interpretation: Cohen's d expresses the difference between the two means in terms of standard deviations. Here's a general interpretation of the values of Cohen's d:

- 0.2: Small effect size (the difference between the two groups is small).
- 0.5: Medium effect size (the difference is moderate).
- 0.8: Large effect size (the difference is substantial).

Assessing Practical Significance*:* While statistical significance indicates whether an effect exists, Cohen's d helps determine the **magnitude** or **practical significance** of the effect, which is crucial for understanding the real-world implications of research findings.

Meta-Analysis*:* Cohen's d is widely used in meta-analyses to aggregate and compare the effect sizes from multiple studies, providing a more comprehensive understanding of an intervention's effectiveness.

3.2.2.4 When to Use:

Cohen's d is appropriate in the following scenarios:

Comparing Two Groups: When you want to quantify the difference between two independent groups, such as in experiments comparing a treatment group to a control group.

Pre-Post Studies: It can also be used to measure the effect size in pre-post study designs where the same participants are measured before and after an intervention.

Meta-Analysis: Cohen's d is often used to combine effect sizes from different studies in a meta-analysis, especially when the studies measure outcomes on different scales.

Assessing the Impact of Interventions: In educational research, psychology, medicine, and social sciences, Cohen's d helps determine the effectiveness of interventions or treatments.

3.2.3 Standard Error (SE)

Using the Cohen's d, the formula is shown below:

$$\boldsymbol{S\,E_d} = \sqrt{\frac{(\boldsymbol{n1}+\boldsymbol{n2})}{\boldsymbol{n1}\,\boldsymbol{x}\,\boldsymbol{n2}} + \frac{\boldsymbol{d^2}}{\boldsymbol{2}\,\boldsymbol{x}\,(\boldsymbol{n1}+\boldsymbol{n2})}} \qquad (3)$$

Where:

- ***n1***: Sample size of Group 1.
- ***n2***: Sample size of Group 2.
- ***d*****:** Cohen's d, which is the effect size.
- **SE**$_d$: Standard error of Cohen's d.

3.2.3.1 Explanation:

The first part of the formula: $\sqrt{\frac{(\boldsymbol{n1}+\boldsymbol{n2})}{\boldsymbol{n1}\,\boldsymbol{x}\,\boldsymbol{n2}}}$, accounts for the inverse of the total sample size and its distribution across the two groups.

The second part of the formula: $\sqrt{\frac{d^2}{2\,x\,(n1+n2)}}$, adjusts for the effect size itself, correcting for bias in smaller samples.

3.2.3.2 Purpose:

The standard error of Cohen's d provides a measure of the precision of the effect size estimate. It tells you how much the observed effect size is expected to vary from the true effect size in the population.

3.2.3.3 When to Use:

In Meta-Analysis*:* When pooling effect sizes from multiple studies, you need the SE of Cohen's d to weight the studies appropriately.

In Reporting*:* When reporting Cohen's d as an effect size, the SE gives additional context about the reliability of that effect size.

3.2.4 Variance

This refers to the variance of the Effect Size. It is a measure of the spread or dispersion of a set of data points around their mean. It quantifies the extent to which the data points differ from the mean value. In the context of effect sizes, particularly Cohen's d, variance indicates the degree of uncertainty or variability in the estimate of the effect size.

The variance of an estimate (for Cohen's d) is related to the standard error (SE) by the following relationship:

$$\textbf{Variance} = \boldsymbol{S\,E^2} \qquad (4)$$

It is simply the square of the standard error to get the variance.

Where:

- ***Variance****:* Variance of Cohen's d.

- SE^2*:* Standard error of Cohen's d.

3.2.4.1 Explanation:

Standard Error (SE): The standard error represents the average amount by which the estimated effect size (Cohen's d) is expected to differ from the true effect size in the population. It reflects the precision of the estimate.

Variance: Since variance is the square of the standard error, it provides a measure of how spread out the estimated effect sizes are expected to be due to sampling variability. Variance gives us the squared measure of this dispersion.

- **Low Variance:** Indicates that the effect size estimate is precise, with little variation expected if the study were repeated multiple times.
- **High Variance:** Indicates greater uncertainty in the effect size estimate, meaning that the observed effect size could fluctuate more widely around the true effect size in the population.

3.2.4.2 Purpose:

Variance serves to quantify the variability in the effect size estimate, helping researchers understand the reliability of their findings. It is particularly useful in the following contexts:

Assessing Estimate Precision: Variance helps in determining how precise an effect size estimate is, with lower variance indicating higher precision.

Constructing Confidence Intervals: Variance is used to calculate the range within which the true effect size is likely to fall (confidence intervals).

Weighting in Meta-Analysis: In meta-analyses, studies with lower variance (and thus higher precision) are given more weight when combining effect sizes from multiple studies.

3.2.4.3 When to Use:

In Reporting Effect Sizes: Understanding variance helps to interpret the reliability of the effect size estimate.

In Meta-Analysis: Variance is crucial for appropriately weighting studies based on the precision of their effect size estimates.

In Hypothesis Testing: Variance is used to assess the significance of the observed effect size relative to a null hypothesis.

3.2.5 Weight

In the context of Cohen's d, especially in meta-analysis, the weight assigned to an individual study reflects the study's contribution to the overall pooled effect size estimate. Studies with more precise (less variable) effect size estimates are given more weight because they provide more reliable information about the true effect size.

3.2.5.1 Formula.

This is the inverse variance weighting.

$$\mathbf{Weight} = \frac{\mathbf{1}}{\mathbf{Variance}} \tag{5}$$

Where:

- ***Weight****:* Weight of the study.
- ***Variance****:* Variance of Cohen's d.

3.2.5.2 Explanation:

Higher Weight: A study with a smaller variance (and therefore a smaller standard error) will have a higher weight, meaning it will have a greater influence on the pooled effect size in a meta-analysis. This is because a smaller variance indicates a more precise estimate of the effect size.

Lower Weight: Conversely, a study with a larger variance (and therefore a larger standard error) will have a lower weight, indicating that its estimate is less precise and thus should have less influence on the overall effect size.

3.2.5.3 Purpose:

The purpose of assigning weights in meta-analysis is to combine effect sizes from multiple studies in a way that gives more influence studies with more reliable estimates. This approach leads to a more accurate and meaningful pooled effect size, reflecting the best available evidence.

Pooling Effect Sizes: Weighted averaging of effect sizes ensures that more precise studies have a greater impact on the overall conclusions.

Reducing Bias: By weighting studies appropriately, you reduce the influence of less precise or outlier studies, leading to more robust meta-analytic findings.

3.2.5.4 When to Use:

In Meta-Analysis: When combining effect sizes from multiple studies, weights are crucial for calculating a pooled effect size that accurately reflects the precision of each study's estimate.

Reporting Combined Results: In any analysis where multiple estimates are aggregated, weights ensure that the most reliable data are emphasised.

3.3 Key Features of Meta-Analysis

3.3.1 Systematic Literature Review

A meta-analysis begins with a systematic review of relevant literature. This involves identifying a specific research question, selecting studies that meet predefined inclusion and exclusion criteria, and collecting data on outcomes, methodologies, and variables from each

study. The systematic review ensures that the meta-analysis is comprehensive and minimises bias.

3.3.2 Quantitative Synthesis

Meta-analysis goes beyond qualitative synthesis by employing statistical methods to combine the results of individual studies. Effect sizes are calculated for each study, which are then aggregated to produce a pooled effect estimate. This enables researchers to determine the overall magnitude of an effect or relationship across the included studies.

3.3.3 Identifying Patterns and Variability

Meta-analysis helps in identifying consistent patterns or trends in research, as well as explaining heterogeneity or variability in study results. This is particularly important in fields like cybersecurity professionalisation, where studies may differ in their methodologies, populations, or definitions of key concepts.

3.3.4 Addressing Publication Bias

One of the key strengths of meta-analysis is its ability to address publication bias. By including both published and unpublished studies, and by assessing the potential for bias (e.g., through funnel plots or statistical tests), meta-analyses can provide a more accurate and less biased estimate of the true effect.

3.3.5 Generalisability and Robustness

Meta-analyses improve the generalisability of research findings by synthesising data from multiple studies across different contexts. The aggregated results provide stronger evidence than a single study, which may be limited by sample size, geographic location, or other contextual factors.

3.4 Applications in Cybersecurity and Professionalisation

In the context of cybersecurity and professionalisation, meta-analysis is useful for evaluating:

3.4.1 Effectiveness of training programs

Meta-analyses can compare the outcomes of different cybersecurity training programs and frameworks, identifying which approaches lead to the most significant improvements in skills and knowledge.

3.4.2 Global professionalisation efforts

Meta-analyses can help synthesise data on professionalisation frameworks across various fields (e.g., law, healthcare, IT) and apply the findings to develop a unified cybersecurity professionalisation framework.

3.4.3 Challenges and barriers

By pooling evidence from multiple studies, meta-analysis can identify the most common challenges, such as fragmentation in certification systems or lack of standardisation, providing actionable insights for addressing these issues.

3.5 Meta-Analysis Steps

The specific steps in this meta-analytic approach include:

3.5.1. Defining Study Questions

The primary study questions guiding the meta-analysis are:

3.5.2 What are the key success factors and common challenges in the Defining Study Questions

The primary study questions guiding the meta-analysis are:

1. What are the key success factors and common challenges in the professionalisation frameworks of various professions?

2. How can these insights inform the development of a professionalisation framework for cybersecurity?

3.5.3 Data Collection

The data collection process is critical to ensure that only high-quality, relevant studies are included in the study. This process involves multiple stages to systematically identify, evaluate, and select the appropriate literature, guided by a clear search strategy and defined inclusion and exclusion criteria. Data collection involves identifying, selecting, and reviewing relevant literature. The process includes:

3.5.3.1 Literature Search: The literature search will be comprehensive, involving academic databases and search engines such as ERIC, ProQuest, Google Scholar, Researchgate and JSTOR. These databases cover a wide range of disciplines and offer access to peer-reviewed articles, conference papers, books, and reports. Using multiple databases ensures a broad search that captures relevant studies across different fields and regions.

Keywords will play a pivotal role in locating relevant literature. Some of the key terms include “professionalisation or professionalization,” and terms that are specific to professional fields such as “healthcare”, “legal”, “education” “engineering,” and “cyber security”. Combining these keywords with Boolean operators (e.g., AND, OR) will help refine search results to capture studies that align with the research objectives. Additionally, using advanced search features like filtering by date or source type will narrow down results to peer-reviewed, contemporary literature.

The search will also be iterative, where initial searches may identify additional relevant keywords or concepts, leading to subsequent, more refined searches.

Furthermore, manual searches in reference lists of identified key articles will help uncover additional sources.

3.5.3.2 Inclusion Criteria:

Studies will be included if they: Examine the professionalisation of a specific profession: Studies will be selected if they focus on professional fields with well-established frameworks or those that are relevant to cybersecurity. Professions such as healthcare, legal, education and engineering are chosen because they have established professionalisation processes, including certification, licensure, and ethical standards. Examining these fields provides a very strong foundation for comparative analysis with cybersecurity field.

Provide empirical evidence on success factors and challenges: Only studies that offer measurable outcomes or qualitative insights into the professionalisation process will be included. Empirical studies, both qualitative and quantitative, provide the needed evidence-backed insights into factors that promote or hinder professionalisation. This ensures the research is grounded in real-world data rather than relying on theoretical or speculative discussions.

Are peer-reviewed and published within the last 20 years: In this study, peer-reviewed articles ensure credibility and rigor, as they have been evaluated by experts in the field. The study limits the search to publications from the last 20 years ensures that the findings truly reflect current trends, challenges faced, practical issues and practices in professionalisation. This is particularly important in current fast-evolving fields like IT and cybersecurity, where technological advancements continue to evolve and would continuously update in professional standards and practices.

3.5.3.3 Exclusion Criteria:

Studies will be excluded if they: Do not provide empirical data: Studies that are solely theoretical or conceptual without backing by empirical research (e.g., opinion pieces, editorials, speculative discussions) will be excluded. While theoretical discussions can offer important insights, the focus of this research is on real-world applications and measurable outcomes.

Are not peer-reviewed or fail to meet academic standards: Non-peer-reviewed sources such as magazine articles, blogs, and white papers from commercial organisations will be excluded. These sources may lack the rigorous review process that ensures reliability and objectivity, which is essential for producing robust research findings.

Focus on professions with no clear parallels to cybersecurity: The inclusion of professions like engineering, healthcare, IT, and law ensures that the professionalisation processes studied are applicable or adaptable to cybersecurity. Studies focusing on professions that are too niche or not analogous to cybersecurity (e.g., professions without formal licensure or certification processes) will be excluded to maintain the relevance of the analysis to the field of cybersecurity.

3.5.4 Data Extraction

Once the relevant studies are selected through the inclusion and exclusion criteria, a systematic data extraction process will be conducted. This step ensures that all necessary information is collected consistently and efficiently across the selected studies. A standardised data extraction form will be used to gather detailed information, allowing for accurate comparisons and synthesis of the data.

The data extracted will include:

3.5.4.1 Study Details:

For each study, the following bibliographic information will be collected:

Title: The title of the study provides a concise summary of the research focus.

Authors: Identifying the authors helps in tracking contributions from specific experts or research groups.

Year of publication: The year allows tracking the recency of the study and ensures relevance to current professionalisation trends, especially for rapidly evolving fields like IT and cybersecurity.

Journal: The journal in which the study was published will be noted to assess the academic rigor and credibility of the source, as peer-reviewed journals tend to have stricter quality controls than non-peer-reviewed outlets. This information also aids in understanding the disciplinary focus of the study (e.g., technology, education, healthcare).

Field: The "Field" column categorises each study by the specific professional domain it examines, such as engineering, law, healthcare, IT, or cybersecurity. This classification helps contextualise the study's findings within its industry, making it easier to compare and apply insights to the professionalisation of cybersecurity. It also allows for the identification of trends and challenges specific to each field, contributing to a more tailored approach when developing a cybersecurity professionalisation framework.

3.5.4.2 Professionalisation Elements:

This section will capture specific elements of professionalisation (see Table 4) addressed by each study, focusing on the mechanisms through which professional status is achieved and maintained in various fields.

Table 4

Success and Challenge Factors in Professionalisation Frameworks

Success Factors	Challenges
1. Standardised education and certification ensure consistency (Cooklev, 2010).	1. Fragmentation in certification systems leads to inconsistency (Spinner, 2010).
2. Ethical guidelines enforced by regulatory bodies (Cameron, 2000).	2. Resistance to standardisation due to regional differences (ÓhÉigeartaigh,, 2020).
3. Continuous Professional Development (CPD) keeps professionals up to date (Dymock & Tyler, 2018).	3. Lack of ethical oversight weakens the profession's credibility (Shoaib et al., 2024).
4. Global standardisation and mutual recognition facilitate cross-border mobility (Washington Accord, 2021).	4. Occupational Closure and Exclusion that creates barriers for qualified individuals to enter the profession (Evetts, 2013).
5. Strong industry-academia collaboration ensures alignment between educational outcomes and industry needs (Janssens, 2013)	5. Rapid technological change makes government workforce training ineffective as compared to private training (Kim & Park, 2020).
6. Implementation of a comprehensive cybersecurity body of knowledge standardises education and practice across the field (Gunther, 2014)	6. Fragmented State of Cybersecurity Body of Knowledge. (Rashid et al., 2018).
7. Investment in cybersecurity training and awareness programs strengthens workforce capabilities (Taherdoost, 2024)	7. Cybersecurity Workforce Skills Gaps (Skill Framework) and Ongoing Challenges. (ISC2, 2023)

These elements will include:

Certification Processes: The study's exploration of how professional certification or licensure is established and maintained in the field. For example, studies that focus on IT certifications like CompTIA A+, SANS certifications for Cybersecurity (Andersson & Reimers, 2009) or healthcare licenses for medical practitioners will be reviewed to understand how these processes ensure competency and professionalism.

Ethical Standards: Ethical guidelines and frameworks that guide professional behavior. This could include codes of ethics, professional responsibility, and standards of practice, which ensure that professionals uphold certain moral and ethical responsibilities.

Continuous Professional Development (CPD): The requirements and structures for ongoing education and training that professionals must engage in to maintain their certification or stay current in their field. This element is critical in fast-evolving fields like cybersecurity, where the threat landscape changes rapidly.

Regulatory Frameworks: The role of regulatory bodies or government agencies in overseeing and enforcing professional standards. This could include national boards (e.g., medical boards, bar associations) or international standards organisations (e.g., ISO standards for cybersecurity).

3.5.4.3 Success Factors:

This section will extract data on the success factors identified in the studies. These are the elements that contribute to the effective professionalisation of a field. For example:

Strong regulatory oversight: The presence of regulatory bodies is crucial for the professionalisation of any field. These organisations establish and enforce professional standards, ensuring that practitioners meet minimum competency requirements. For example, in the healthcare sector, medical boards regulate the licensure of doctors, mandating continuous education and adherence to ethical guidelines.

Regulatory oversight helps maintain public trust and ensures that professionals are held to high standards of practice. In fields like engineering and law, regulatory bodies often set the criteria for licensure and certification, oversee examinations, and monitor compliance with professional codes of conduct, thereby protecting the integrity of the profession and safeguarding public interest.

Industry Recognition: Industry recognition of certifications is vital for the legitimacy and success of professionalisation efforts. When employers and industry stakeholders accept and value certifications as a mark of expertise, it reinforces the importance of obtaining and maintaining these credentials.

This recognition often leads to better job opportunities, career advancement, and higher remuneration for certified professionals. For instance, certifications like PMP (Project Management Professional) in project management or CISSP (Certified Information Systems Security Professional) in cybersecurity are widely recognised and sought after by employers, which motivates professionals to pursue and maintain these credentials.

Industry recognition also drives the demand for standardised training and education programmes that prepare candidates for certification.

Clear Competency Frameworks: In well-defined and structured competency frameworks, it is essential for guiding the proper education, competency-based training, and professional development of individuals within a field. For the benefit of the profession, these frameworks outline the importance of knowledge, skills, and abilities required for various roles and career stages, providing a structured pathway for upgrading and professional growth.

For example, the engineering profession often relies on detailed competency models that specify the technical competency and soft skills necessary for different levels of practice, from entry-level as engineers and all the way up to senior professionals. Another example, the information security or cybersecurity professions adopted frameworks that are used to improve human resource functions and education, aiming to help to narrow the skills gap from which the profession is suffering (Bendler

& Felderer, 2023). With clear competency frameworks, they ensure consistency in the quality of professionals entering the workforce and help to align educational programmes with the industry needs, thus facilitating the professionalisation process.

Accessible Certification and CPD Programmes: Certification processes and continuous professional development (CPD) programmes must be widely accessible and relevant to the current demands of the industry. Accessibility includes factors such as affordability, availability in different geographic regions, and the flexibility to accommodate professionals' varying schedules.

For example, online certification programmes and CPD courses allow professionals to upskill without the need to take extended time off work. Moreover, these programmes need to stay current with industry trends and emerging technologies to ensure that the skills being taught are applicable to the challenges professionals face today.

Affordable and accessible certification and CPD opportunities encourage more professionals to engage in lifelong learning, which is critical for maintaining competence in rapidly evolving fields like IT and cybersecurity.

Collaborations Between Academia and Industry: Partnerships between educational institutions and industry are essential for aligning training and education with the practical skills required in the workforce. These collaborations ensure that curricula are updated to reflect the latest industry practices and technologies, and that students gain relevant, hands-on experience before entering the job market.

For example, in the field of IT, partnerships between universities and tech companies can result in internship opportunities, co-developed courses, and guest lectures from industry professionals. Such collaborations help bridge the gap between

theory and practice, ensuring that graduates are well-prepared to meet the demands of their chosen profession.

Additionally, these partnerships can lead to the development of specialised certification programmes that are recognised and valued by both academia and industry, further supporting the professionalisation process.

3.5.4.4 Challenges:

This section will identify the challenges and obstacles faced in the professionalisation process across different professions. These might include:

Rapid technological changes: Rapid technological advancements pose significant challenges to maintaining up-to-date certification standards and curricula, particularly in fields like IT and cybersecurity. As new technologies emerge, they introduce novel risks and require professionals to continuously update their skills.

For instance, the rise of artificial intelligence (AI) and quantum computing has necessitated the development of new cybersecurity strategies and tools, which in turn demands that educational and certification bodies swiftly adapt their offerings to include these emerging technologies. However, the speed at which technology evolves often outpaces the ability of certification bodies to update their standards, leading to a lag in the relevance of certifications.

This challenge is particularly acute in the cybersecurity profession, where the cyber threat landscape evolves quickly and changes rapidly, thus it highlights the importance of the requirements to be constant vigilance and the frequent overhaul of educational content for the cyber practitioners to stay current and relevant.

Lack of Industry-Standard Certifications: In some professions, the absence of universally recognised certifications can hinder professionalisation efforts by creating a

fragmented landscape of standards. Without a centralised or widely accepted certification system, professionals may face inconsistencies in the quality and recognition of credentials across different regions or industries.

For example, in cybersecurity, there are multiple certifications available, such as CISSP, CISM, and CEH, each recognised differently depending on the region or employer. This lack of standardisation can lead to confusion among employers and employees alike, potentially diluting the value of certifications and hindering the establishment of a cohesive professional identity.

Moreover, without universally recognised certifications, it becomes challenging to ensure that all professionals meet a consistent standard of competency, which is crucial for maintaining public trust and ensuring the effectiveness of the profession.

Cost and Accessibility of Certifications: The cost and accessibility of certification and training programs can significantly limit participation, especially in developing regions or among professionals with limited financial resources. High costs associated with certification exams, preparatory courses, and continuous professional development (CPD) can create barriers for individuals seeking to enter or advance in a profession.

Additionally, geographical accessibility is a major concern, as professionals in remote or underserved areas may not have easy access to testing centres or training facilities. This limitation is particularly problematic in global fields like IT and cybersecurity, where the demand for certified professionals is high, but the opportunity to obtain these credentials may be unevenly distributed.

Reducing the cost and increasing the accessibility of certification programs is essential to promoting inclusivity and ensuring a diverse, well-prepared professional workforce.

Resistance to Change: Resistance to change is a common challenge in professions with established traditions and long-standing practices. This resistance can come from practitioners who are accustomed to traditional methods or from institutions that are reluctant to overhaul existing standards and curricula.

In fields like law or medicine, where professional standards have been in place for decades, introducing new certification requirements or updating competency frameworks to include emerging skills can be met with scepticism or outright opposition. This resistance can slow the adoption of necessary changes, ultimately hindering the profession's ability to adapt to new challenges and technologies.

In cybersecurity, where rapid change is the norm, overcoming this resistance is crucial for ensuring that professionals are equipped with the latest knowledge and skills to effectively combat evolving threats.

Inconsistent Global Standards: Inconsistent global standards in certification requirements and professional qualifications present significant challenges to the global recognition of credentials. In today’s interconnected world, professionals often work across borders, and consistent standards are essential for ensuring that their qualifications are recognised and respected internationally.

However, differences in certification processes, regulatory requirements, and professional standards across countries can create barriers to mobility and collaboration. For example, a cybersecurity professional certified in one country may find that their credentials are not recognised in another, limiting their career opportunities and complicating efforts to address global cybersecurity challenges.

Harmonising standards across regions and establishing mutual recognition agreements between countries could help alleviate these issues, promoting a more cohesive global professional community.

By systematically extracting this information, the review will be able to compare and contrast the elements that contribute to successful professionalisation in various fields. The goal is to identify key insights that can inform the development of a robust professionalisation framework for cybersecurity. This data extraction process will also facilitate a clear understanding of both the enablers and barriers to effective professionalisation across professions

3.6 Inclusion and Exclusion Criteria

To ensure the quality and relevance of the studies included in the meta-analysis, the following inclusion and exclusion criteria (see Tables 5 and 6) will be applied:

3.6.1 Inclusion Criteria:

Studies that focus on professionalisation in established fields such as engineering, law, healthcare, and IT.

- This criterion ensures that the study includes professions that have a clear history of establishing competency frameworks, professional codes of conduct, and certification standards. For instance, the professionalisation of engineering is well-documented through organisations like the IEEE and the use of licensure exams (e.g., PE exams in the U.S.).
- Similarly, law and healthcare professions (e.g., bar associations, medical boards) have long-standing systems for professional regulation and continuing education. Including these fields helps draw relevant parallels to the evolving field of cybersecurity, where professional standards are still emerging.

- Studies focused on these established fields can offer insights into how they have managed to set up, maintain, and update their professionalisation frameworks in response to industry changes and technological advancements.

Empirical studies that provide measurable outcomes or qualitative insights into professionalisation success factors and challenges.

- This criterion emphasises the importance of including studies that not only discuss professionalisation conceptually but also provide real-world, evidence-based findings. Empirical studies that present measurable outcomes, such as pass rates of professional certification exams, or qualitative insights, such as interviews with professionals about the barriers to entering their fields, will be key.
- Such studies can highlight important factors like the role of ongoing education, certification requirements, or the establishment of ethical standards in professional growth and recognition.
- For instance, success factors may include the development of standard competencies and certification exams, while challenges could involve keeping certifications up-to-date in fast-changing fields like IT and cybersecurity.

Studies published in peer-reviewed journals from year 2005 onwards, ensuring that the study reflects current trends and challenges.

- The focus on peer-reviewed journal publications from year 2005 onwards ensures the inclusion of high-quality, rigorously reviewed academic work.
- This time frame captures the most relevant trends and developments in professionalisation, as many industries—including IT, healthcare, and law—have undergone significant transformation due to globalisation, technological advancements, and the increasing complexity of regulatory environments.

- Furthermore, this time frame will capture shifts in professionalisation driven by digital transformation, such as the growing need for continuous professional development in response to emerging technologies and cybersecurity threats.

Table 5

Selection Criteria for Empirical Journal Articles

Inclusion Criteria	Description
1. General	- Contents should be relevant to the research objective and questions - Contents should provide clear insights to the research context. - Suitable metho adapted for the research questions
2. Focus on Professionalisation in Established Fields	- Studies must focus on professionalisation in established fields. - Studies have competency frameworks, codes of conduct, and certification standards. - Studies offer insights into how professionalisation frameworks are developed, maintained, and updated.
3. Empirical Focus	- Studies should provide empirical evidence. - Studies should have measurable outcomes or qualitative insights.
4. Peer-Reviewed Publications and Currency	- Studies must be published in peer-reviewed journals - Studies must be published from 2005 onwards - Studies to reflect current trends and challenges in professionalisation.
5. Findings	- The research findings should provide adequate data analysis and presentation - Findings should be coherent and logically tied to the research data.
6. Conclusions	- The studies should address the core research questions and provide clear recommendations. - The studies should offer actionable strategies

3.6.2 Exclusion Criteria:

Studies that focus solely on theoretical or conceptual discussions without providing empirical evidence.

- This exclusion criterion ensures that the review does not include studies that lack a practical or evidence-based approach. Theoretical papers, while valuable for understanding frameworks and abstract concepts, do not provide measurable outcomes or actionable insights that can be applied to real-world professionalisation efforts.
- In the context of cybersecurity, where the field is rapidly evolving, empirical data (e.g., studies on the effectiveness of certification programs or professional development initiatives) is crucial to understanding what works in practice.
- This exclusion ensures that the focus remains on studies that provide tangible, evidence-backed contributions to professionalisation discussions, offering more reliable conclusions.

Articles that are not peer-reviewed or are published in non-academic sources.

- This criterion ensures the inclusion of high-quality and rigorously reviewed research. Peer-reviewed articles have undergone critical scrutiny by experts in the field, which increases the credibility and reliability of the findings.
- Non-peer-reviewed sources, such as blogs, news articles, or reports from commercial entities, may lack the objectivity or methodological rigor required for academic studies. By excluding these sources, the review maintains a focus on scholarly work that has been vetted for accuracy and relevance.
- This is particularly important in a field like cybersecurity, where there is a proliferation of commercially driven content, which may not provide unbiased insights into professionalisation practices.

Studies that are overly specialised or specific to a niche area without broader applicability to the professionalisation of cybersecurity.

- This exclusion criterion aims to filter out studies that focus on very narrow, specialised areas that do not have a broader impact on professionalisation in cybersecurity.
- For instance, a study examining a niche topic such as "the professionalisation of cryptography within a small academic community in a specific country" may provide limited relevance to the larger question of professionalisation across the cybersecurity industry.
- By excluding overly specialised studies, this criterion ensures that the included research addresses issues, trends, or frameworks that are broadly applicable across various subfields of cybersecurity. This helps ensure the findings can inform broader strategies for the professionalisation of cybersecurity as a whole.

Table 6

Exclusion Criteria of Journal Articles

Inclusion Criteria	Description
1. General Criteria	- The content is irrelevant and inadequate to the topic of professionalisation.
2. Theoretical or Conceptual Focus	- Studies that focus only on theoretical or conceptual discussions. - No practical or measurable outcomes. - Non evidence-based studies.
3. Studies Overly Specialised or Niche	- Studies highly specialised or niche without broader relevance to cybersecurity.

3.7 Data Analysis

The data extracted from the selected studies will undergo a structured analysis to identify patterns in success factors and challenges across different professions. The analysis process includes the following steps:

3.7.1 Thematic Coding:

The data will be analysed using thematic coding, a qualitative method that involves identifying recurring themes across multiple studies (Braun & Clarke, 2006). Success factors, such as standardised education and ethical guidelines, will be coded as separate themes, while challenges like fragmentation in certification systems will be coded similarly. This will help to organise the data into meaningful categories.

3.7.2 Aggregation of Findings:

After coding the data, findings will be aggregated to identify the most common factors contributing to the success or challenge of professionalisation frameworks. Quantitative data (e.g., the percentage of professions using certification systems) will be summarised, and qualitative data (e.g., descriptions of ethical enforcement challenges) will be synthesised to draw general conclusions.

3.7.3 Comparison Across Professions:

The aggregated findings will be compared across professions to identify differences and similarities in professionalisation efforts. For example, the role of regulatory bodies in enforcing ethical standards in healthcare will be compared to similar efforts in engineering or law. This cross-professional comparison will help to determine which factors are most relevant to the professionalisation of cybersecurity.

3.7.4 Application to Cybersecurity:

The final step in the data analysis process is to apply the identified success factors and challenges to the context of cybersecurity. The insights gained from other professions will inform the development of a professionalisation framework that addresses the unique needs and challenges of the cybersecurity field. This includes designing standardised certification processes, establishing ethical guidelines, and promoting continuous professional development (CPD).

3.8 Ethical Considerations

As this study relies on the analysis of existing literature, there will be no direct interaction with individuals, and no new data collection will be conducted that involves human subjects. As such, ethical concerns are minimal.

However, the author will ensure that all studies reviewed are properly cited and that the analysis is conducted in a way that accurately reflects the original authors' contributions. The use of peer-reviewed literature ensures the reliability and validity of the sources used.

Given the nature of this study, informed consent from participants is not applicable, and no participant-related risks or ethical concerns are anticipated (see Appendix E).

3.9 Limitations

While the meta-analysis approach provides a robust method for synthesising findings from multiple studies, several limitations must be acknowledged that may impact the overall conclusions of this study:

3.9.1 Availability of Data:

- The availability and quality of relevant studies may significantly limit the scope and depth of the meta-analysis. While professionalisation is well-documented in fields like engineering, law, and healthcare, there may be fewer studies on

emerging fields such as cybersecurity, especially those that meet the inclusion criteria of being empirical and peer-reviewed.

- In newer fields like cybersecurity, the body of literature may be fragmented or nascent, which could affect the ability to make broad generalisations or identify trends across the profession. Additionally, studies in rapidly evolving fields may become outdated quickly, posing challenges in gathering recent, relevant data.
- This limitation may lead to gaps in understanding how professionalisation is progressing in cybersecurity, compared to more established fields with longer histories of professional development and certification.

3.9.2 Diversity of Professions:

- While examining multiple professions (e.g., law, engineering, healthcare, IT) provides valuable comparative insights, the differences between these fields could pose challenges in drawing direct parallels to cybersecurity.
- Each profession has unique regulatory environments, cultural practices, competency frameworks, and professional standards. For example, the professionalisation of law involves licensing and bar examinations, which may not have direct equivalents in cybersecurity. Similarly, healthcare's reliance on strict licensure and ethical standards may not fully map onto the cybersecurity field, where certification is still voluntary in many regions.
- Therefore, while the comparison of various fields is insightful, the heterogeneity of the professions being studied might require adjustments or interpretations to make the findings applicable to cybersecurity. This challenge could limit the direct applicability of the findings without further contextualisation specific to the cybersecurity domain.

3.9.3 Subjectivity in Thematic Coding:

- The process of thematic coding involves interpreting data to identify recurring themes, and while efforts will be made to minimise bias, the potential for subjectivity cannot be entirely eliminated.
- Thematic analysis is inherently subjective, and while methodological rigor (e.g., using a coding framework, cross-checking themes) will be applied, there remains a risk that different researchers might interpret themes differently.
- For example, what one researcher views as a "challenge" in professionalisation (e.g., slow adoption of certification standards) may be interpreted by another as an opportunity for improvement. Additionally, in fields like cybersecurity, where rapid technological changes occur, the subjective interpretation of themes such as “continuous professional development” might vary depending on the context or specific professional framework being discussed.
- This introduces the risk of inconsistencies in thematic coding, despite attempts to standardise the process, potentially affecting the comparability of the results.

To address these limitations, efforts will be made to ensure methodological rigor, such as expanding the search for relevant studies, contextualising findings from different professions, and employing techniques like inter-rater reliability in thematic coding to reduce bias. However, the inherent limitations of the meta-analysis approach must be acknowledged, particularly in the context of emerging fields like cybersecurity.

3.10 Summary

This chapter has detailed the comprehensive methodology employed in this study, focusing on the use of meta-analysis to examine and compare professionalisation frameworks

across various well-established professions. The approach leverages both qualitative and quantitative data from a wide array of fields—such as engineering, law, healthcare, and IT—in order to identify and extract relevant insights that can inform the development of a cybersecurity-specific professionalisation framework.

The data collection process is structured to ensure a systematic and rigorous review of the literature, encompassing multiple academic databases to capture a broad spectrum of research. By applying stringent inclusion and exclusion criteria, the study ensures that only empirical, peer-reviewed studies are included, with a focus on professionalisation mechanisms such as certification processes, ethical standards, regulatory frameworks, and continuous professional development (CPD). This careful selection process guarantees that the studies reviewed reflect the most current and relevant trends in professionalisation across multiple industries.

The analysis phase will focus on identifying key success factors and challenges observed in the professionalisation efforts of these established professions. Success factors such as the development of clear competency frameworks, strong industry recognition, and accessible certification pathways will be highlighted as essential elements for creating a sustainable professionalisation process. Simultaneously, common challenges, such as rapid technological advancements, resistance to change, and inconsistent global standards, will be carefully considered to address potential obstacles in cybersecurity.

The findings from these diverse professions will then be synthesised and adapted to address the specific needs and unique characteristics of the cybersecurity field. Given the rapid pace of technological innovation, as well as the increasing complexity and specialisation within cybersecurity, it is essential that any professionalisation framework proposed for this field is flexible, adaptive, and future proof. Drawing lessons from more established professions ensures

that the cybersecurity framework will incorporate tried-and-tested strategies, while also being tailored to the specific challenges of cyber defense, information security, and risk management.

Ultimately, this study will propose a comprehensive framework that not only supports the standardisation of professional competencies in cybersecurity but also promotes the ongoing development and recognition of professionals within this critical and fast-evolving domain. This framework aims to align with global trends and best practices, ensuring that cybersecurity professionals are well-equipped to meet the demands of an increasingly complex and interconnected world.

Chapter 4. Results

4.0 Summary of Key Themes from Chapters 1-3

Chapter 1 sets the foundation of the study by highlighting the need for a globally recognised professionalisation framework for the cybersecurity profession. As cyber threats grow, a structured and standardised approach to certifying cybersecurity professionals is crucial to ensuring consistent skill levels, credibility, and global mobility. The study draws on insights from established professions such as engineering, law, and healthcare, which have developed effective professionalisation frameworks. The objectives include identifying key success factors and challenges in these fields and applying them to cybersecurity.

Chapter 2 reviews professionalisation frameworks across multiple fields. In engineering, the Washington Accord has facilitated global standardisation, while healthcare and law benefit from strong ethical guidelines and regulatory oversight. Continuous professional development (CPD) plays a critical role in maintaining professional competence in fast-evolving fields like healthcare. However, challenges like fragmented certification systems, resistance to standardisation, and lack of ethical oversight hinder professionalisation in IT and cybersecurity. The chapter identifies both success factors, such as global standardisation, and challenges, like the fragmentation of certification systems.

Chapter 3 outlines the meta-analysis approach used to synthesise data from 20 peer-reviewed studies on professionalisation frameworks across various professions. The methodology includes a systematic review of studies that focus on success factors and challenges in professionalisation efforts. The inclusion criteria ensure that relevant and empirical studies from year 2005 onwards are examined. Data extraction focuses on identifying common themes, including certification processes, ethical standards, and CPD, and these insights are applied to the design of a cybersecurity professionalisation framework. The chapter

also discusses the limitations, such as variability in available data and potential subjectivity in thematic coding.

These chapters collectively provide the foundation for understanding how professionalisation in other fields can inform the development of a comprehensive and standardised framework for cybersecurity professionals.

4.1 Introduction

This chapter presents the results of the meta-analysis conducted on the professionalisation frameworks across various established professions, including engineering, law, healthcare, and information technology (IT). The results focus on identifying the success factors and challenges observed in the professionalisation efforts of these fields. These findings are then synthesised to provide insights into how these factors can inform the development of a comprehensive professionalisation framework for the cybersecurity profession. The results are organised around key themes that emerged from the analysis of the selected studies.

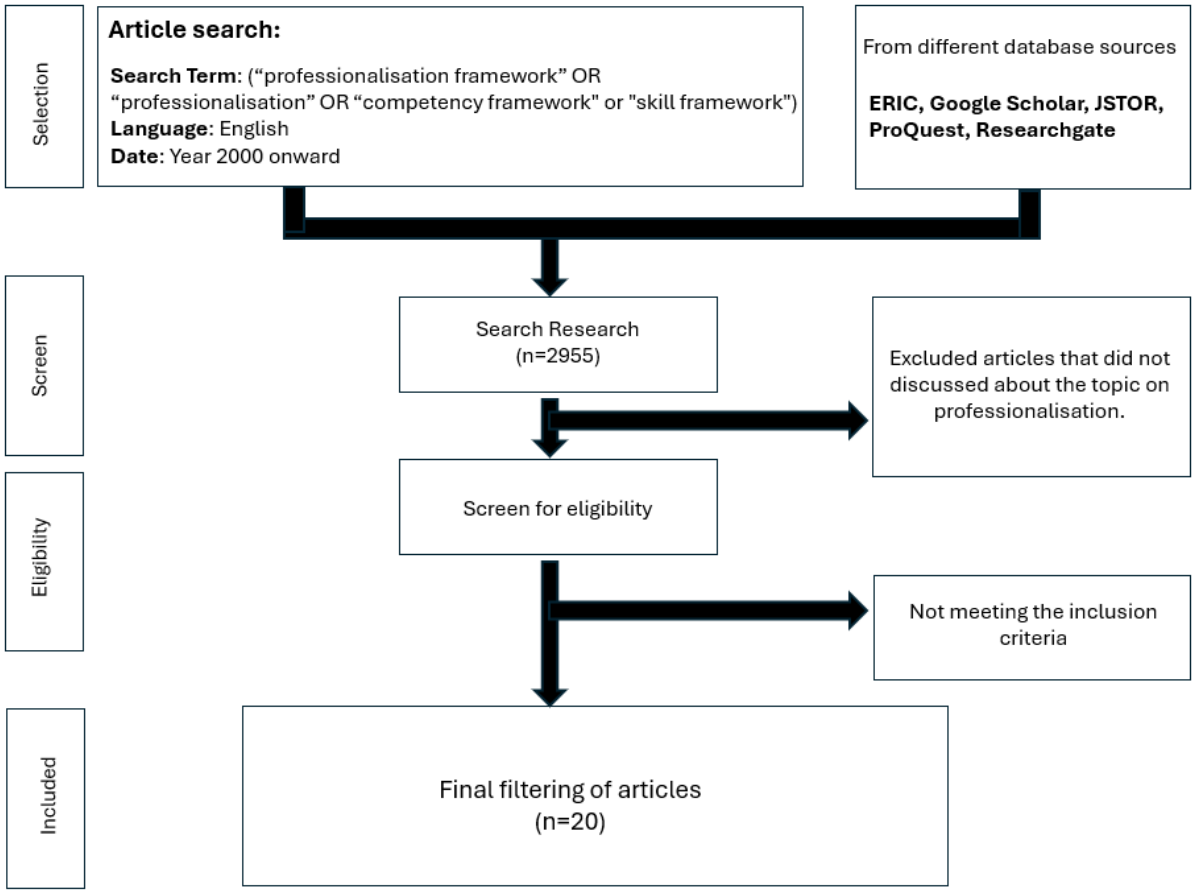
4.2 Selection of Relevant Professionalisation Frameworks

In this meta-analysis, the study selection process (see Figure 2) begins with defining clear inclusion and exclusion criteria to determine which studies will be considered.

Figure 2

Flowchart of the Selection Strategy for the Meta-Analysis

(based on Tseng et al., 2016, p.2)



A comprehensive literature search (see Table 7) is then conducted across multiple databases to gather potential studies. Key words such as "professionalisation frameworks" or "professionalisation" or "competency framework" together with the boolean operators (e.g. AND, OR) to refine the search.

Table 7

The Search Terms Used to find the Peer-Reviewed Articles

Online Databases or Platforms	**Search Terms**	**Articles identified.** **Size = n**
ERIC	(professionalisation or professionalization) AND (healthcare or legal or education or engineering or cybersecurity)	1814

Online Databases or Platforms	**Search Terms**	**Articles identified.** **Size = n**
Google Scholar	"professionalisation" or "professionalization" AND "healthcare" or "legal" or "education" or "engineering" or "cybersecurity"	20
JSTOR	((professionalisation or professionalization) AND (healthcare or legal or education or engineering or cybersecurity))	0
ProQuest	professionalisation or professionalization AND healthcare OR legal OR education OR engineering OR cybersecurity	1090
Researchgate	professionalisation or professionalization AND healthcare OR legal OR education OR engineering OR cybersecurity	31
Total		2955

For ERIC and ProQuest searches, we further refine the search criteria, with addition search terms such as “competency framework” or “skill framework” to reduce the number of articles. At the end of these searches, the titles, abstracts, and publication from year 2005 onward of these studies (see Table 8) are screened to exclude irrelevant ones. The remaining studies undergo a full-text review to confirm their eligibility.

Table 8

Parameters for Searching of Journal Articles

Parameters	Inclusion Criteria
1. Access Rights	The full text can be accessed or downloaded.
2. Language	The literature is available in English.
3. Publication information	The publication provides clear details about the author, institution, or organisation, as well as the publication date

Parameters	Inclusion Criteria
4. Published Post-2005	The information was published and made available online from the year 2005 onward.
5. Subject matter	The publication includes either an independent professionalisation framework or one that integrates with skills or competency models, such as job roles, certification processes, ethical standards, continuous professional development, or regulatory frameworks.
6. Subject matter	The competency model outlines the key competencies that practitioners or graduates from higher education institutions should possess.

We ended the search and filtering, and eventually found around 20 peer-reviewed studies at the end of the selection exercise. Relevant data is then extracted from the selected studies. Finally, a quality assessment is performed to evaluate the risk of bias and overall quality of the studies included in the analysis.,

4.3 Overview of Studies Included in the Meta-Analysis

The meta-analysis included a total of 20 peer-reviewed studies published between 2005 and 2024, focusing on professionalisation frameworks or key elements related to professionalisation frameworks in the fields of engineering, law, healthcare, and IT. The studies were selected based on their relevance to the study objectives, which were to identify the critical success factors and challenges in professionalisation efforts and apply these findings to cybersecurity.

The selected studies were drawn from academic databases such as ERIC, ProQuest, Google Scholar, Researchgate and JSTOR (see Table 9), and they provided both qualitative and quantitative data. The majority of the studies examined professionalisation within a specific national or regional context, while a few explored global frameworks, such as the Washington Accord for engineering or international standards in healthcare.

4.4 Peer-Reviewed Studies

The meta-analysis included twenty (20) peer-reviewed articles (see Table 9) that were published between years 2005 and 2024. These studies focused on topics or important elements related to professionalisation frameworks across various fields such as engineering, law, healthcare, and information technology (IT). The studies were selected based on their relevance to the study objectives, providing insights into the success factors and challenges in professionalisation processes.

Table 9

Details of the 20 Peer-Reviewed Articles Included in the Meta-Analysis

Title	Author(s)	Year of Publication	Journal	Field
1. Medical Ethics: A Distinctive Species of Ethics	Fleck, L. M. (2020)	2020	Cambridge Quarterly of Healthcare Ethics	Healthcare
2. The role of standards in engineering education	Cooklev, T. (2010)	2010	International Journal of IT Standards and Standardization Research	Engineering
3. The professionalisation of information security: Perspectives of UK practitioners	Reece, R. P. (2015)	2015	Computers & Security	Cybersecurity
4. How to maneuver in the world of negative online reviews, the important ethical considerations for attorneys, and changes needed to protect the legal profession	Goodrum, A. (2015)	2015	Information & Communications Technology Law	Law
5. Transnational Authority in the Knowledge-Based Economy: Who Sets the Standards of ICT Training and Certification?	Graz & Hartmann (2012)	2012	International Political Sociology	IT
6. Strategic professional development	Senior, C. (2009)	2009	International Journal of Continuing Engineering	Engineering

Title	Author(s)	Year of Publication	Journal	Field
			Education and Life-Long Learning	
7. The Professionalization of Compliance: Its Progress, Impediments, and Outcomes.	Fanto, (2021)	2021	Notre Dame Journal of Law, Ethics & Public Policy	Law
8. The ethics of ethical regulation: Protecting the practitioner as well as the client.	Gunther, S. V (2014)	2014	Psychotherapy and Politics International,	Healthcare
9. All that glitters is not gold: On the effectiveness of cyber security qualifications	Knowles et al. (2017)	2017	Computer	Cybersecurity
10. Innovative Proposed Model between Formative Research and Accreditation of Engineering Programs	Andrade-Arenas et al., (2023)	2023	Communications of the ACM	Engineering
11. A Principlist framework for cybersecurity ethics	Formosa et al. (2021)	2021	Computers & Security	Cybersecurity
12. Continuing professional development in the legal profession: A practice-based learning perspective	Gold, et al. (2007)	2007	Management Learning	Law
13. Elevating IT's professional status	Ko. C. (2009)	2009	ComputerWorld Hong Kong	IT
14. No quick fix: A sustainable solution to lab personnel shortages	Cilia, K. (2023)	2023	Medical Laboratory Observer (MLO)	Healthcare
15. A step towards the Washington Accord (1989)?	Ooi, K. B. (2006)	2006	International MultiConference of Engineers & Computer Scientists	Engineering
16. Ethics and the law: An introduction	Dare, T. (2016)	2016	Legal Ethics	Law
17. The Gap between Perceived Value of Information Technology Certification and the Persistence Applied to Achieve Such Certification	Udeh, I. E. (2016)	2016	International Journal of Business Research & Information Technology	IT
18. Looking to Other Professions to Advance the	Jankowski et al. (2020)	2020	American Journal of Bioethics	Healthcare

Title	Author(s)	Year of Publication	Journal	Field
Health Care Ethics Consultant Certification Program				
19. What Competencies Should Undergraduate Engineering Programs Emphasize? A Systematic Review	Passow & Passow (2017)	2017	Journal of Engineering Education	Engineering
20. Cybersecurity Frameworks and Models: Review of the Existing Global Best Practices	Shukla et al. (2024)	2024	Productivity	Cybersecurity

These 20 studies included in this meta-analysis provide a comprehensive view of professionalisation efforts across multiple fields. These studies examine key elements (see Table 10) such as certification systems, ethical guidelines, continuous professional development (CPD), and regulatory frameworks, offering valuable insights for the professionalisation of the cybersecurity profession. The findings from these studies are critical in identifying both the success factors and challenges that need to be considered when developing a global, standardised cybersecurity framework.

Table 10

The Success and Challenge Identified in the Meta-Analysis

Author(s)	Success Factors	Challenge Factors
1. Fleck, L. M. (2020)	Ethical standards in healthcare	Maintaining ethical oversight across different regions
2. Cooklev, T. (2010)	Global standardisation of engineering education	None identified
3. Reece, R. P. (2015)	Recognised cybersecurity certifications	Fragmentation in certification systems
4. Goodrum, A. (2015)	Ethical guidelines in law	Resistance to global standardisation
5. Graz & Hartmann (2012)	Standardisation in IT certifications	Fragmentation in IT professional certifications

Author(s)	Success Factors	Challenge Factors
6. Senior, C. (2009)	Continuous Professional Development in engineering	Implementation of CPD across regions
7. Fanto, (2021)	Mutual recognition in law	Limited mutual recognition due to jurisdictional differences
8. Gunther, S. V (2014)	Regulatory frameworks in healthcare	Challenges in maintaining consistent regulation
9. Knowles et al. (2017)	Evolution of IT professionalisation	Lack of cohesive global certification systems
10. Andrade-Arenas et al., (2023)	Accreditation in engineering	Difficulties in maintaining global mobility standards
11. Formosa et al. (2021)	Cybersecurity certification ethics	Ethical oversight challenges in certification bodies
12. Gold, et al. (2007)	CPD in law	Challenges in enforcing continuous education requirements
13. Ko. C. (2009)	Professionalisation in IT	Inconsistent professional standards across regions
14. Cilia, K. (2023)	Healthcare certification	Regulatory challenges in healthcare certification oversight
15. Ooi, K. B. (2006)	Global standardisation in engineering	None identified
16. Dare, T. (2016)	Ethics in the legal profession	Enforcement of ethical guidelines across jurisdictions
17. Udeh, I. E. (2016)	Fragmentation in IT certifications	Difficulty in achieving certification cohesion
18. Jankowski et al. (2020)	Ethical oversight in healthcare	Lack of consistent cross-country regulation
19. Passow & Passow (2017)	Success of the Washington Accord in engineering	None identified
20. Shukla et al. (2024)	Cybersecurity professionalisation	Fragmented certifications and lack of global standardisation

Table 11

The New Factors Identified in the Meta-Analysis

Author(s)	New Opportunities	Description
1. Fleck, L. M. (2020)	Cross-Discipline collaboration	Fosters collaboration across disciplines like law, psychology, and business.
2. Cooklev, T. (2010)	Nil	Nil
3. Reece, R. P. (2015)	Cybersecurity bills	Proposes legislative measures for cybersecurity governance and regulations.
4. Goodrum, A. (2015)	Code of Conduct	Establishes ethical standards for cybersecurity professionals.
5. Graz & Hartmann (2012)	Technical Skills and Competency Levels	Defines clear competency levels for technical cybersecurity skills.
6. Senior, C. (2009)	Lifelong Learning and Availability	Encourages continuous learning and adaptation in the evolving cybersecurity field.
7. Fanto, (2021)	Professional Licensing	Introduces licensing requirements for cybersecurity professionals.
8. Gunther, S. V (2014)	Regulatory Framework	Promotes regulatory frameworks for healthcare compliance.
9. Knowles et al. (2017)	Job Roles and Career Pathways	Advocates for clear career paths and defined job roles in cybersecurity.
10. Andrade-Arenas et al., (2023)	Unified Body of Knowledge	Standardizes the body of knowledge in cybersecurity across different regions.
11. Formosa et al. (2021)	Diversity and Inclusion in Cybersecurity	Strengthens ethical guidelines for cybersecurity certification processes.
12. Gold, et al. (2007)	Lifelong Learning and Availability	Promotes continuous education enforcement in the legal sector.
13. Ko. C. (2009)	Professional Associations' Role in Professionalisation	Promotes unified professional standards across IT sectors.
14. Cilia, K. (2023)	Regulatory Framework	Facilitates cross-country regulatory frameworks in healthcare certification.
15. Ooi, K. B. (2006)	Nil	Nil.
16. Dare, T. (2016)	Code of Conduct	Enhances global ethical standards in the legal profession.

Author(s)	New Opportunities	Description
17. Udeh, I. E. (2016)	Technical Skills and Competency Levels	Harmonises technical certification across fragmented IT sectors.
18. Jankowski et al. (2020)	Practice Insurance	Promotes cross-country insurance policies for cybersecurity practice.
19. Passow & Passow (2017)	Nil	Nil
20. Shukla et al. (2024)	Adoption and Translation of Body of Knowledge	Facilitates adoption of cybersecurity knowledge across different regions.

Table 12

The Study Data

Study	Effect Size	Standard Error	Variance	Weight
1. Fleck, L. M. (2020)	0.55	0.061	0.003721	268.744961
2. Cooklev, T. (2010)	0.823	0.045	0.002025	493.8271605
3. Reece, R. P. (2015)	0.733	0.051	0.002601	384.4675125
4. Goodrum, A. (2015)	0.822	0.057	0.003249	307.7870114
5. Graz & Hartmann (2012)	0.583	0.022	0.000484	2066.115702
6. Senior, C. (2009)	0.818	0.068	0.004624	216.2629758
7. Fanto, (2021)	0.667	0.058	0.003364	297.2651605
8. Gunther, S. V (2014)	0.789	0.043	0.001849	540.8328826
9. Knowles et al. (2017)	0.806	0.056	0.003136	318.877551
10. Andrade-Arenas et al., (2023)	0.701	0.065	0.004225	236.6863905
11. Formosa et al. (2021)	0.758	0.041	0.001681	594.8839976
12. Gold, et al. (2007)	0.577	0.023	0.000529	1890.359168
13. Ko. C. (2009)	0.771	0.066	0.004356	229.5684114
14. Cilia, K. (2023)	0.845	0.033	0.001089	918.2736455
15. Ooi, K. B. (2006)	0.899	0.045	0.002025	493.8271605
16. Dare, T. (2016)	0.543	0.048	0.002304	434.0277778
17. Udeh, I. E. (2016)	0.678	0.067	0.004489	222.7667632

Study	Effect Size	Standard Error	Variance	Weight
18. Jankowski et al. (2020)	0.698	0.054	0.002916	342.9355281
19. Passow & Passow (2017)	0.899	0.077	0.005929	168.6625063
20. Shukla et al. (2024)	0.583	0.044	0.001936	516.5289256

Note:

a. **Effect size**: Effect size is a quantitative measure of the magnitude of a phenomenon. It describes the strength of the relationship between two variables or the extent of an experimental effect.
b. **Standard error**: is the standard deviation of the sampling distribution of a statistic, most commonly the mean.
c. **Variance**: measures the spread of a set of numbers. Specifically, it is the average of the squared differences from the mean.
d. **Weight**: In the context of meta-analysis, weight refers to the relative importance of each study's results in the overall analysis.

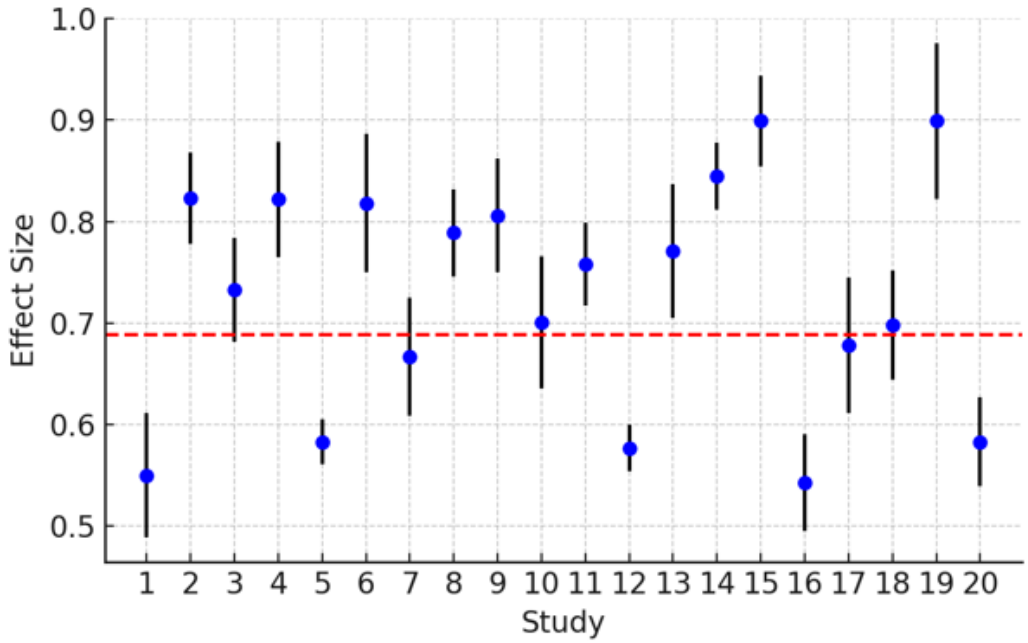
4.4.1 The Forest Plot of Effect Sizes

The forest plot displays the individual effect sizes of the 20 studies (see Figure 3), along with their 95% confidence intervals (Borenstein et al., 2009). The red dashed line represents the overall weighted mean effect size calculated from all studies.

The forest plot from this dataset provides strong evidence that the intervention or treatment studied across these 20 studies generally has a positive and significant effect. The consistency in the effect sizes, with most falling in the medium to large range, coupled with the relatively narrow confidence intervals in many studies, underscores the robustness of these findings. The moderate heterogeneity observed suggests that while there are some differences across studies, these do not undermine the overall conclusion that the treatment is effective.

Figure 3

The Forest Plot of Effect Sizes



Note:

Components of the plot:

a. **X-Axis:** The x-axis lists the studies included in the meta-analysis, numbered from1 to 20.
b. **Y-Axis:** The y-axis represents the effect size of each study.
c. **Blue Dots (Effect Sizes):** Each blue dot represents the **effect size estimate** for an individual study included in the meta-analysis.
d. **Black Lines (Confidence Intervals):** The black lines extending from each blue dot represent the 95% confidence intervals for the effect size of that study. A longer line indicates greater uncertainty in the estimate.
e. **Red Dashed Line**: The red dashed line represents the overall weighted mean effect size across all studies, which is approximately 0.7 in this plot.

Thee effect size tells us how strong or significant the findings are in each study. Plotting studies against their effect sizes helps us see the differences in results across multiple studies. This comparison shows not just whether an effect exists, but also how big that effect is in each study, helping us understand the overall trend or impact across all the studies.

4.4.2 Interpretation

4.4.2.1 Variation in Effect Sizes: The effect sizes across the studies vary, with some studies reporting higher or lower effects (<0.7) than the overall mean. This variation is expected in meta-analyses, especially when the studies differ in design, sample size, or population.

4.4.2.2 Interpretation of Variation

Heterogeneity: The variation in effect sizes among the studies indicates some degree of heterogeneity. Some studies (e.g., studies 1, 12, and 16) show effect sizes well below 0.7, while others (e.g., studies 2, 13, 18) show effect sizes closer to or above 0.8. This spread suggests that not all studies agree on the effect size, which could be due to differences in study design, populations, or other factors.

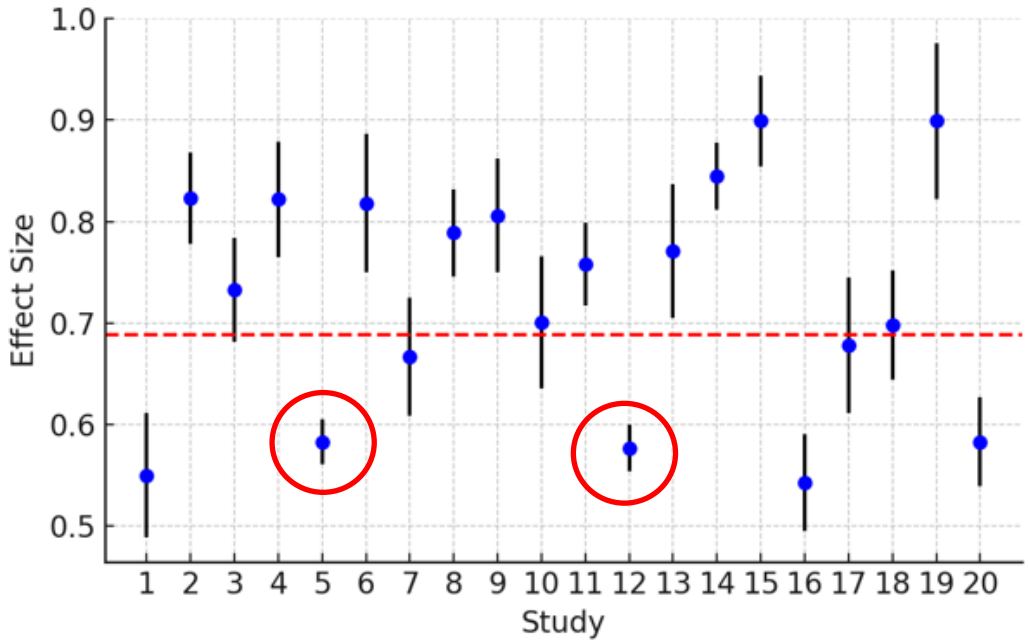
Confidence Intervals Crossing the Overall Effect: Some studies have confidence intervals that cross the red dashed line, meaning their effect sizes are not significantly different from the overall effect (e.g., studies 6, 9, 14). This implies that these studies' results are consistent with the overall meta-analytic result.

Outliers: A few studies may be considered outliers with effect sizes and confidence intervals that do not overlap with the overall effect size (e.g., study 19 with a high effect size and study 16 with a lower effect size).

4.4.2.3 Precision of Studies: Studies with narrower confidence intervals (shorter horizontal lines such as study 5 and study 12, see Figure 4) are more precise, likely due to larger sample sizes. These studies contribute more to the overall weighted mean effect size.

Figure 4

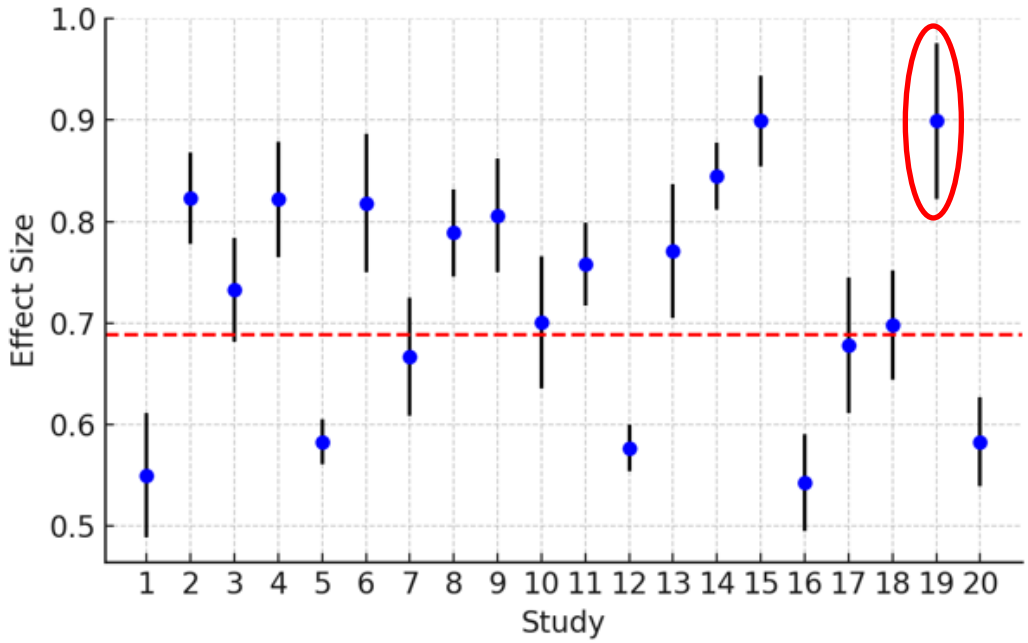
The Forest Plot of Effect Sizes – Narrower Confidence Interval



4.4.2.4 Significance: Most of the studies have confidence intervals that do not cross the vertical line at zero, suggesting that these studies report statistically significant effects. A few studies have wider intervals (e.g. study 19, see Figure 5), indicating less precision in the effect size estimate due to smaller sample sizes or more variability in the data.

Figure 5

The Forest Plot of Effect Sizes – Wider Confidence Interval

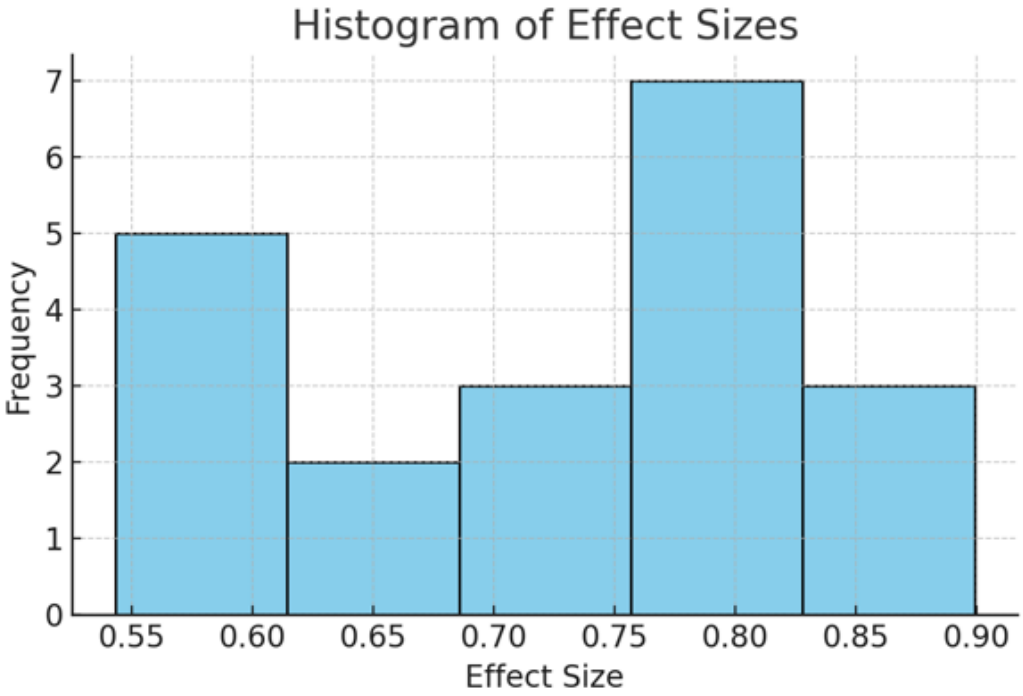


4.4.3 Histogram of Effect Sizes

The histogram illustrates the distribution of effect sizes across the 20 studies (see Figure 6). The histogram of effect sizes (Borenstein et al., 2009) provides a clear and compelling visual representation of the consistency and magnitude of the effect sizes reported across the 20 studies in this dataset. The concentration of effect sizes in the medium to large range, without significant skewness or outliers, suggests that the intervention is consistently effective across different contexts and study designs. This uniformity strengthens the conclusions drawn from the meta-analysis, indicating that the treatment or intervention has a substantial and reliable impact across various studies.

Figure 6

The Histogram of Effect Sizes



Note: Frequency tells us how often something happens, like counting how many times an event occurs. Effect size shows us how strong or big the difference or relationship is between things. Frequency gives us the "how often," while effect size gives us the "how much." Together, they help us understand both the occurrence and the impact of an event.

4.4.4 Interpretation

4.4.4.1 Central Tendency: The effect sizes are generally clustered around the weighted mean effect size, with most studies reporting medium to large effect sizes (between approximately 0.55 and 0.9). This suggests that the treatment or intervention examined in these studies consistently shows a substantial impact.

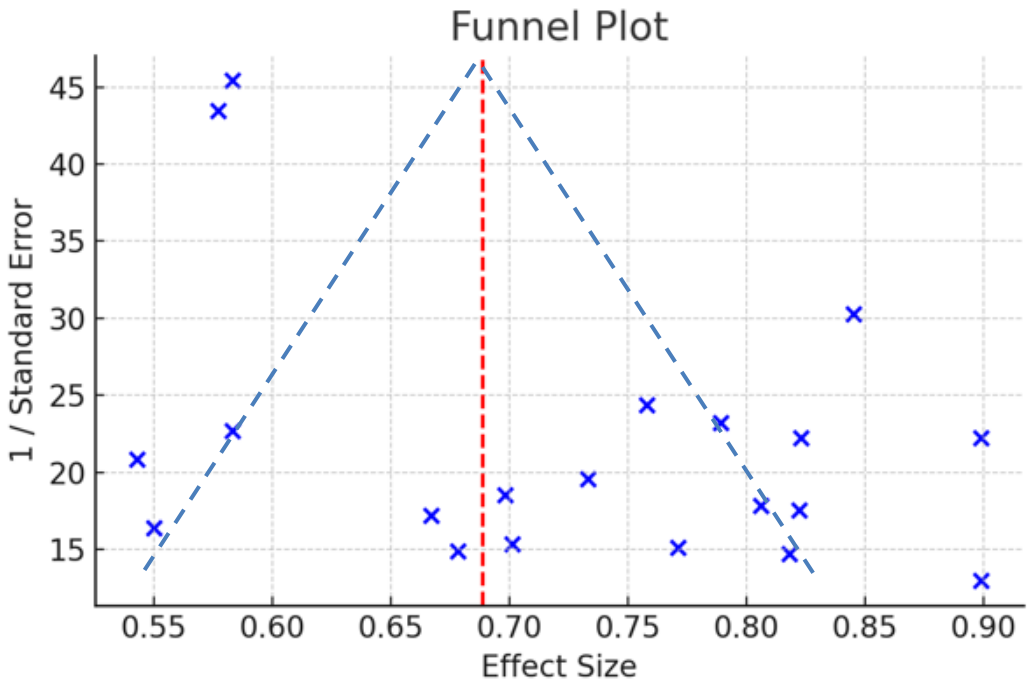
4.4.4.2 Variability: The distribution is fairly concentrated, indicating that most studies report similar effect sizes. There are no extreme outliers, which suggests a degree of consistency in the results across the studies.

4.4.5 Funnel Plot (Publication Bias Check)

The funnel plot (see Figure 7) provides a visual check for publication bias and an understanding of the distribution of study results in relation to their precision (Light & Pillemer, 1984). Based on this dataset, the funnel plot helps to ensure that the meta-analysis results are not skewed by selective reporting. If the plot is symmetrical and forms a clear funnel shape, it suggests that the studies included in the analysis represent a balanced view of the evidence, supporting the reliability of the overall conclusions. Conversely, any asymmetry could point to the need for caution in interpreting the results, as it might suggest that the meta-analysis is influenced by the selective publication of studies with more favourable outcomes.

Figure 7

The Funnel Plot



Note: Inverse of variance (1/variance) is used to determine how much weight each study should have in calculating the overall effect size. Studies with smaller variance (more precise estimates) are given more weight because they provide more reliable information. Effect size measures the strength or magnitude of the effect being studied. By using 1/variance to weight the effect sizes, the meta-analysis emphasises the results of studies that are more precise, leading to a more accurate overall estimate of the effect.

4.4.6 Interpretation

4.4.6.1 Symmetry: The points in the funnel plot should ideally form an inverted funnel shape around the overall effect size. If the plot is symmetrical, this suggests no significant publication bias.

4.4.6.2 Potential Bias: If there's asymmetry, where studies are missing on one side of the plot (especially with smaller studies clustering on one side), it could indicate publication bias. In this case, if the plot is relatively symmetrical, it suggests that there may not be a significant publication bias, meaning that both significant and non-significant results have likely been reported.

4.4.6.3 Study Distribution: If most studies cluster closely around the mean effect size, it indicates a consistent effect size, but if there is a spread, it suggests variability in study precision.

4.4.6.4 Analysis & Interpretation: In this case, the points on the left side of the mean effect size (indicated by the red dashed line) are fewer and less dispersed compared to those on the right side. There seems to be a greater spread of points on the right side of the mean, particularly at lower levels of precision (toward the bottom of the plot).

The funnel plot does not appear to be perfectly symmetrical, as more studies are clustered on the right side, with a broader spread. This might suggest some level of asymmetry.

The possible cause of this asymmetry effect in a funnel plot could indicate publication bias, where studies with smaller or non-significant effects are less likely to be published, or it could reflect genuine heterogeneity among the studies (differences in study populations, interventions, or methodologies).

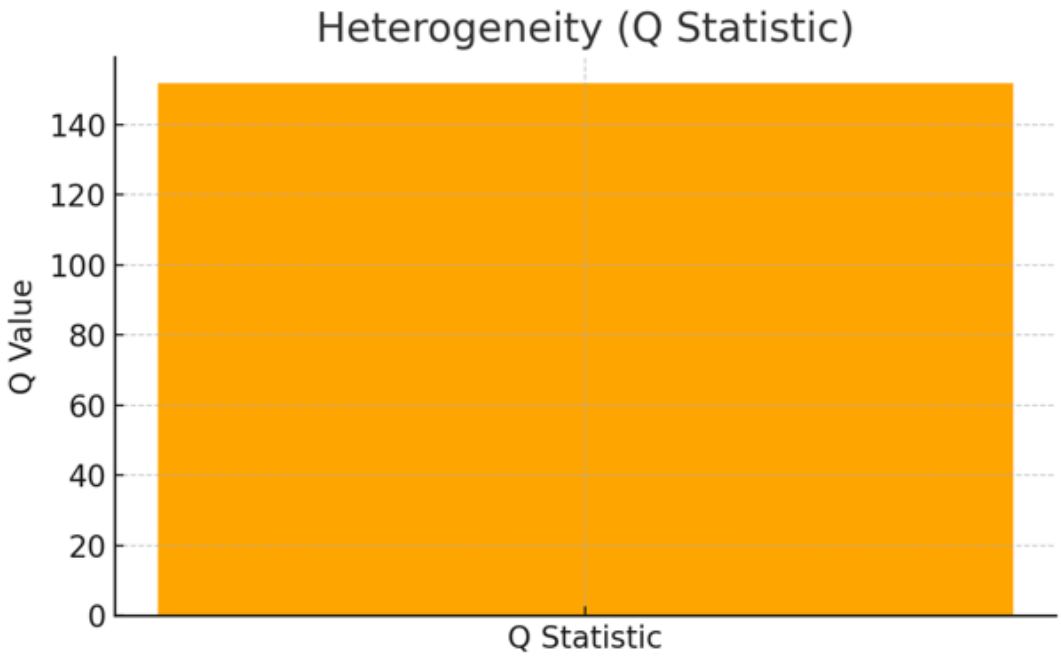
4.4.7 Bar Chart of Q Statistic (Heterogeneity)

The bar chart displays the Q statistic (see Figure 8), which measures the heterogeneity across the studies (Hedges & Olkin, 1985). In this research, the high Q statistic suggests significant heterogeneity among the professionalisation frameworks across the professions studied. The substantial variability indicates that the differences in the success and failure rates of these frameworks are likely due to actual differences in how these frameworks are implemented and contextual factors unique to each profession, rather than random chance.

Given the high Q statistic, it provides an opportunity for further research to use a random-effects model (Borensteain et al., 2010) in the meta-analysis to account for the variability between professions, rather than assuming a common effect size across all studies. This finding implies that the professionalisation frameworks should be analysed with consideration for the unique context and implementation strategies in each profession.

Figure 8

The Heterogeneity (Q Statistic) Chart



4.4.8 Interpretation:

4.4.8.1 High Q Statistic: The plot above shows a high Q statistic (around 140) indicates that there is significant heterogeneity among the studies, meaning that the variability in effect sizes is greater than what would be expected by chance. This suggests that the studies may differ in terms of populations, interventions, or methodologies, leading to varying results.

4.4.8.2 Low Q Statistic: A lower Q statistic would indicate homogeneity, where the studies are more consistent in their results.

4.4.8.3 Heterogeneity in This Analysis: If the Q statistic in the bar chart is high, it suggests that there is considerable variability in the effect sizes, which could warrant a random-effects model (Borenstein et al., 2009) for more accurate meta-analysis. This would mean that the studies are not all estimating the same underlying effect size, possibly due to differences in study design or populations.

4.4.9 Summary of Effect Size and Statistics of the Studies

The overall effect size and statistics (See Table 13):

Table 13

Overall Effect Size and Statistics

Description	Metric Value
1. Weighted Mean Effect Size	0.688661173
2. 95% Confidence Interval (CI) Lower	0.669924787
3. 95% Confidence Interval (CI) Upper	0.707397559
4. Q Statistic	151.7738257

4.4.10 Summary of the Metric Values

4.4.10.1 Weighted Mean Size: The weighted mean effect size represents the average effect size across all the studies included in the meta-analysis. The weighting typically gives more importance to studies with larger sample sizes or more precise estimates. Here, the average effect size is approximately 0.689. This value suggests that, on average, the studies show a moderate effect in the direction being measured.

4.4.10.2 95% Confidence Interval (CI): The 95% confidence interval provides a range within which the true mean effect size is likely to fall, with 95% confidence. In this case, the true effect size is likely between 0.670 and 0.707. This narrow interval suggests that the estimated effect size is relatively precise. The fact that the entire confidence interval is above zero indicates that the effect is statistically significant.

4.4.10.3 Q Statistic: The Q statistic is a measure of heterogeneity, which indicates whether the effect sizes from the different studies are consistent with each other. A higher Q statistic suggests greater variability among the effect sizes than would be expected by chance alone. In this case, a Q statistic of 151.774 may indicate significant heterogeneity, suggesting that the effect sizes across the studies vary more than would be expected if they were all estimating the same effect. This could imply that different studies are measuring slightly different effects or that there are other factors influencing the results.

4.4.11 Overall Interpretation

The meta-analysis reveals a moderate and statistically significant effect size (approximately 0.689) with a narrow confidence interval, indicating that the results are likely reliable. However, the relatively high Q statistic suggests there may be variability between the study results, indicating the need to explore potential sources of heterogeneity or consider using random-effects models to account for this variation.

4.4.11.1 Consistency and Precision: The forest plot and histogram suggest that while there is some variability in effect sizes, most studies report medium to large effects, and many of them are fairly precise (narrow confidence intervals). This points to a generally consistent and significant effect across the studies.

4.4.11.2 Publication Bias: The funnel plot provides some reassurance that publication bias may not be a significant issue, as there is no pronounced asymmetry in the plot.

4.4.11.3 Heterogeneity: The Q statistic suggests there might be moderate to significant heterogeneity among the studies. This would imply that a random-effects model is more appropriate for this meta-analysis, allowing for the variability across studies to be accounted for in the final effect size estimate.

4.5 Thematic Analysis

In this study, thematic analysis is a qualitative research method used to identify, analyse, and report patterns (themes) within data (Braun & Clarke, 2006). It involves a systematic process of coding the data, grouping codes into themes, and then interpreting the meaning of those themes in the context of the research question. This method helps in uncovering insights and understanding complex phenomena by organising and simplifying large volumes of data.

4.5.1 Thematic Table

The thematic table (see Table 14) which is a structured representation of the themes and sub-themes identified during thematic analysis. It organises the key findings into categories, making it easier to understand and communicate the relationships between different concepts.

4.4.5.1 Thematic Diagram. As for the thematic diagram, it will visually represents the relationships between themes and sub-themes identified in the study. It often takes the form of a network or flowchart, where each theme is connected to its sub-themes, showing how different concepts are related. Thematic diagrams are helpful for illustrating the connections

between themes, making it easier to grasp the overall structure of the findings and to see how different aspects of the data interrelate.

The solid lines and dotted lines in the thematic diagram serve distinct purposes in visually representing the relationships between themes and sub-themes. A solid line in a thematic diagram suggests that the two connected elements have a significant and unambiguous relationship. This could be a causal link, a dependency, or a flow of influence. A dotted lines represent indirect, secondary, or weaker relationships between themes and sub-themes. They indicate a connection that exists but is either less direct, more complex, or perhaps conditional. It could also indicate that the relationship is more conceptual or potential rather than concrete.

Table 14

Thematic Table: Professionalisation in Cybersecurity

Theme	Sub-theme	Key Points
1. Ethical Standards	Code of Conduct	Establishing ethical guidelines and expectations for cybersecurity professionals
	Ethics Education	Integrating ethics into cybersecurity education and professional development
2. Skills/ Competency Framework	Job Roles and Career Path	Structuring job roles and career progression in cybersecurity
	Soft Skills and Communication	Developing non-technical skills critical for effective teamwork and leadership
	Technical Skills and Competency Levels	Importance of continuous skill development and competency levels
3. Body of Knowledge	Unified Body of Knowledge	Standardising core concepts and practices across the field
	Translation of BoK	Adapting the unified body of knowledge to different contexts and sectors
4. Certification Processes	Cost and Accessibility of Certifications	Addressing financial and logistical barriers to obtaining certifications

Theme	Sub-theme	Key Points
	Certification Renewal	Emphasising the importance of certification and credential in good standing.
5. Factors Inhibiting Professionalisation	Resistance to Standardisation	Challenges in adopting uniform standards across diverse sectors
	Rapid Technological Change	Adapting to new technologies and evolving threat landscapes
	Inconsistent Global Standards	Variability in cybersecurity standards and practices across different countries
	Lack of Ethical Oversight	Variability in enforcing ethical standards across different organisations
	Lack of Mutual Recognition	Challenges in achieving global recognition of certifications across regions
	Fragmentation in Certification Systems	Impact of fragmented certification systems on professional development
	Diversity and Inclusion in Cybersecurity	Promoting diversity and inclusion within the cybersecurity profession
	Fragmentation of body of knowledge	Challenges due to multiple, inconsistent sets of knowledge and practices
6. Regulatory Framework	Regulatory Framework	Establishing laws and regulations such as HIPAA, PCIDSS, SOX, and NIST CSF to professionalise cybersecurity
	Cybersecurity Bills	Legislative measures that regulate cybersecurity practices and compliance
7. Opportunities	Resilience Engineering	Developing systems and processes that enhance the ability to recover from cyber attacks and adapt to future threats
	Sustainable Development	Integrating sustainable practices into cybersecurity to support long-term environmental and societal goals
8. Continuous Professional Development	Lifelong Learning & Adaptability	Emphasising the importance of ongoing learning and skill enhancement throughout a professional's career
9. Professional Associations	Role in Professionalisation	Supporting the formalisation and recognition of the cybersecurity profession

Theme	Sub-theme	Key Points
	Professional Licensing	Ensuring professionals meet established standards through formal certification
	Practice Insurance	Providing protection against legal claims and financial risks in professional practice

The meta-analysis identified all the related factors that have consistently contributed to both the success and challenges of the professionalisation of various professions. Based on this study, a thematic analysis diagram for the cybersecurity professionalisation is proposed (see Appendix D).

4.6 Success Factors Identified

The meta-analysis identified several success factors mentioned in Chapter 2 that have consistently contributed to the effective professionalisation of various professions. The purpose of describing these success factors is to provide a clear and comprehensive understanding of the critical elements that facilitate the development and recognition of a profession. By categorising these success factors into sub-themes, the analysis highlights the key areas that require attention and development to achieve successful professionalisation.

The importance of identifying and understanding these success factors lies in their ability to guide strategic planning and decision-making processes within the field. For stakeholders involved in the professionalisation of a field—whether policymakers, educators, or professional associations—recognising these factors helps in implementing effective strategies that can lead to the formalisation and standardisation of the profession.

The implications for professionalisation are significant and being mentioned too. By addressing and leveraging these success factors, a profession can establish robust frameworks for education, certification, and ethical practice. This not only enhances the credibility and legitimacy of the profession but also ensures that practitioners are adequately equipped to meet

industry demands and societal expectations. Ultimately, the focus on these sub-themes contributes to the sustainability and growth of the profession, positioning it alongside other established and respected fields.

These success factors are categorised into the following sub-themes as follows:

4.6.1 Standardised Education and Certification

4.6.1.1 Description: Standardised education and certification across all professions involve the creation and implementation of uniform educational frameworks and certification processes that apply consistently within a given field. This approach ensures that all professionals within a particular domain receive a consistent level of training and are evaluated against the same criteria, regardless of where or how they obtained their education. The goal is to create a common foundation of knowledge, skills, and ethical standards that every practitioner must meet to be recognised as competent in their profession.

4.6.1.2 Importance: The importance of standardised education and certification across all professions lies in its ability to create a level playing field, ensuring that all practitioners are equipped with the necessary knowledge and skills to perform their roles effectively. This consistency is particularly crucial in professions where the quality of service directly impacts public safety, health, and welfare, such as in healthcare, law, engineering, and cybersecurity. Standardisation helps to maintain high standards across the profession, reducing the risk of errors and inconsistencies that can arise from varied educational backgrounds. Additionally, it provides a reliable benchmark for employers, clients, and regulatory bodies, ensuring that certified professionals are competent and capable of delivering quality services.

4.6.1.3 Implication for Professionalisation: The adoption of standardised education and certification is a fundamental step in the professionalisation of any field. It supports the formal recognition of a profession, establishing it as a distinct and reputable field of expertise. This standardisation also facilitates the development of clear career pathways, allowing professionals to advance based on recognised qualifications and competencies. Furthermore, it enhances the credibility and public trust in the profession, as stakeholders can be confident that all certified practitioners meet the same rigorous standards. By ensuring uniformity in education and certification, the profession can maintain its integrity and continue to evolve in response to changing industry demands and societal needs (Freidson, 2001).

4.6.2 Ethical Guidelines and Regulatory Oversight

4.6.2.1 Description: Ethical guidelines and regulatory oversight across all professions refer to the establishment of universal principles and rules that govern the conduct of professionals and the standards by which they are held accountable. Ethical guidelines provide a framework for decision-making and behaviour, ensuring that professionals act with integrity, respect, and responsibility towards their clients, colleagues, and society. Regulatory oversight, on the other hand, involves the implementation and enforcement of these ethical standards by professional bodies, regulatory agencies, and government entities. This oversight ensures that professionals adhere to the established ethical norms and are held accountable for any deviations.

4.6.2.2 Importance: The importance of ethical guidelines and regulatory oversight in all professions is paramount for maintaining public trust and ensuring the safety, fairness, and effectiveness of professional services. Ethical guidelines are crucial in guiding professionals through complex situations where legal requirements might not

provide sufficient clarity. These guidelines help prevent misconduct, conflicts of interest, and unethical practices that could harm individuals or society. Regulatory oversight ensures that these ethical standards are not merely theoretical but are actively enforced, providing mechanisms for addressing violations and ensuring that professionals are competent and ethical in their practice.

4.6.2.3 Implication for Professionalisation: The establishment of ethical guidelines and regulatory oversight is a cornerstone of the professionalisation process. It contributes to the formal recognition of a profession as a distinct and trusted field of expertise. Ethical guidelines help to define the core values and principles of the profession, promoting a culture of integrity and accountability. Regulatory oversight, meanwhile, reinforces these ethical standards by ensuring compliance and addressing breaches, thus safeguarding the reputation of the profession. Together, ethical guidelines and regulatory oversight help to elevate the profession, enhancing its credibility and fostering public confidence. They also support the continuous improvement of professional standards, as the profession evolves to meet new ethical challenges and societal expectations (Freidson, 2001).

4.6.3 Continuous Professional Development (CPD)

4.6.3.1 Description: Continuous Professional Development (CPD) refers to the ongoing process of learning and skill enhancement that professionals undertake throughout their careers to maintain and improve their competencies. CPD encompasses a wide range of activities, including formal education, workshops, conferences, self-directed learning, and practical experience. The goal of CPD is to ensure that professionals remain up-to-date with the latest developments in their field, adapt to new challenges, and continue to provide high-quality services.

4.6.3.2 Importance: The importance of continuous professional development lies in its ability to keep professionals current and competent in a rapidly changing world. As industries evolve due to technological advancements, regulatory changes, and emerging best practices, CPD ensures that professionals do not become obsolete or stagnant in their knowledge and skills. It fosters a culture of lifelong learning, encouraging professionals to seek out new knowledge, refine their expertise, and stay ahead in their fields. CPD also plays a critical role in maintaining public trust, as it assures clients and stakeholders that professionals are committed to ongoing improvement and are equipped to deliver services that meet contemporary standards.

4.6.3.3 Implication for Professionalisation: Continuous professional development is essential for the professionalisation of any field. It helps to establish a profession as a dynamic and evolving entity, rather than a static body of knowledge. CPD contributes to the formal recognition of a profession by ensuring that its members are consistently competent and knowledgeable, which is crucial for maintaining the profession's credibility and legitimacy. Moreover, CPD supports career progression, enabling professionals to advance within their fields by acquiring new skills and qualifications. This ongoing development fosters a more engaged and motivated workforce, leading to higher standards of practice and greater innovation within the profession (Eraut, 1994).

4.6.4 Global Standardisation and Mutual Recognition

4.6.4.1 Description: Global standardisation and mutual recognition refer to the development and acceptance of uniform standards, practices, and certifications across different countries and regions, along with the mutual recognition of these standards by various professional bodies and regulatory agencies. Global standardisation aims to create a consistent framework for professional qualifications, ethical guidelines, and

best practices, ensuring that professionals from different parts of the world are held to the same standards. Mutual recognition involves the formal agreement between countries or organisations to recognise each other's qualifications and certifications, enabling professionals to practice across borders without the need for redundant re-certification or re-qualification processes.

4.6.4.2 Importance: The importance of global standardisation and mutual recognition lies in their ability to facilitate the mobility of professionals, enhance international collaboration, and ensure that high standards are maintained globally. In an increasingly interconnected world, where professionals often work across borders, having consistent standards helps to ensure that services and practices are of uniform quality, regardless of location. Mutual recognition agreements eliminate barriers to professional mobility, allowing qualified professionals to work internationally, which is particularly important in fields like cybersecurity, engineering, and healthcare. This also helps in addressing skills shortages in various regions by allowing the influx of qualified professionals from other countries.

4.6.4.3 Implication for Professionalisation: Global standardisation and mutual recognition are crucial for the professionalisation of any field on a global scale. By establishing common standards, professions can achieve greater consistency and reliability in the quality of services provided, which enhances public trust and credibility. Mutual recognition further reinforces the profession's status by acknowledging the validity of qualifications and certifications across different jurisdictions, promoting a more integrated and unified professional community. This can lead to the development of global professional networks, increased opportunities for professional growth, and the sharing of best practices across borders. Ultimately, global

standardisation and mutual recognition contribute to the elevation of the profession, positioning it as a cohesive and respected field on the international stage (Sweeney & McFarlin, 2014).

4.7 Challenges Identified

The meta-analysis also revealed several key challenges that have hindered the professionalisation efforts across the different professions as mentioned in Chapter 2. These challenges are especially prevalent in rapidly evolving professions like IT and cybersecurity. The factors are further elaborated, highlighting the importance and implications for professionalisation:

4.7.1 Fragmentation in Certification Systems

A major challenge in the professionalisation of cybersecurity domain is the fragmentation of certification systems. Unlike engineering and healthcare, which have standardised certification processes, IT and cybersecurity are characterised by a multitude of certifications with varying levels of recognition and credibility.

4.7.1.1 Description: In cybersecurity, there may exist a number of certifications that are often overlapping or inconsistent, certification programmes and credentials across the field. This fragmentation is characterised by the lack of a unified framework or standard that aligns these certifications, leading to variations in the content, rigor, and recognition of different certifications. As a result, cybersecurity professionals may face challenges in determining which certifications are most relevant or valued in the industry, while employers may struggle to assess the qualifications of candidates holding different certifications.

4.7.1.2 Importance: The fragmentation in certification systems is a significant issue in cybersecurity because certifications are a primary means of validating a

professional's skills and knowledge. When certification systems are fragmented, it creates confusion among both professionals and employers, potentially leading to gaps in critical skills and inconsistent levels of competency across the workforce. This fragmentation can also result in professionals investing time and resources in certifications that may not be widely recognised or valued, thereby limiting their career progression. Moreover, the lack of standardisation in certifications can undermine efforts to build a cohesive and skilled cybersecurity workforce capable of addressing global cyber threats effectively.

4.7.1.3 Implication for Professionalisation: The fragmentation of certification systems has profound implications for the professionalisation of the cybersecurity field. Professionalisation requires a clear, standardised pathway for education, certification, and career progression. When certification systems are fragmented, it becomes difficult to establish universally accepted standards of practice, which are essential for the recognition and legitimacy of the profession. This fragmentation can hinder the development of a unified professional identity and create barriers to the establishment of global certification standards that ensure consistency in skills and knowledge across the industry. To advance the professionalisation of cybersecurity, there is a need to harmonise certification systems, promoting a more integrated and standardised approach to validating professional competencies (ENISA, 2017).

4.7.2 Resistance to Standardisation

Another significant challenge is the resistance to standardisation observed in fields such as law and cybersecurity. In the legal profession, differences in jurisdictional laws and regulations make it difficult to implement global or even regional professional standards.

Attempts to create unified standards have often met resistance, as legal practitioners are bound by the specific regulations of their respective countries.

4.7.2.1 Description: In cybersecurity, the resistant can stem from various factors, including the desire for flexibility, the complexity of implementing standards in diverse environments, concerns about stifling innovation, or the perception that standardisation may impose undue burdens on organisations. In cybersecurity, where threats are constantly evolving, some stakeholders argue that rigid standards may not keep pace with the dynamic nature of the field.

4.7.2.2 Importance: Standardisation is crucial in cybersecurity because it establishes a common framework for ensuring the security of systems, data, and networks. It helps in creating consistency across different platforms and organisations, enabling interoperability and the effective sharing of information. However, resistance to standardisation can lead to fragmentation, where disparate approaches are taken to address similar security challenges. This lack of uniformity can create vulnerabilities, as attackers may exploit inconsistencies in security measures across different systems. Moreover, without standardisation, it becomes more challenging to assess and compare the effectiveness of security practices, leading to potential gaps in protection.

4.7.2.3 Implication for Professionalisation: Resistance to standardisation has significant implications for the professionalisation of cybersecurity. Professionalisation typically involves the establishment of agreed-upon standards that define the competencies, practices, and ethical guidelines for the profession. Without standardisation, the field of cybersecurity may struggle to achieve a unified identity, making it difficult to create consistent certification processes, educational curricula, and professional codes of conduct. This fragmentation can hinder the recognition of

cybersecurity as a distinct and credible profession, limiting its ability to attract and retain talent. To advance professionalisation, it is essential to overcome resistance to standardisation by demonstrating how consistent practices can enhance security, foster innovation, and support the development of a cohesive professional community (Von Solms & Van Niekerk, 2013).

4.7.3 Lack of Ethical Oversight

4.7.3.1 Description: The lack of ethical oversight in cybersecurity refers to the absence or inadequacy of mechanisms that ensure professionals adhere to ethical standards and principles in their work. Ethical oversight involves the establishment and enforcement of guidelines that govern the conduct of cybersecurity practitioners, ensuring that their actions are aligned with broader societal values and legal frameworks. Without robust ethical oversight, there is a greater risk of unethical practices, such as the misuse of personal data, surveillance without consent, or the development of technologies that could be exploited for malicious purposes.

4.7.3.2 Importance: Ethical oversight is crucial in cybersecurity because professionals in this field often have access to sensitive information and powerful tools that can significantly impact individuals, organisations, and even national security. The lack of ethical oversight can lead to serious consequences, including breaches of privacy, loss of trust in digital systems, and the potential for harm through the misuse of technology. Ethical lapses in cybersecurity can also result in legal penalties, financial losses, and reputational damage for both individuals and organisations. Ensuring that cybersecurity practices are guided by strong ethical principles is essential for maintaining public confidence and protecting the fundamental rights of individuals.

4.7.3.3 Implication for Professionalisation: The absence of ethical oversight poses a significant barrier to the professionalisation of cybersecurity. For a profession to be fully recognised and respected, it must be seen as not only technically competent but also ethically responsible. The establishment of ethical standards and the implementation of oversight mechanisms are key components of this professionalisation process. They help to define the responsibilities of cybersecurity professionals, promote accountability, and ensure that the actions of practitioners contribute positively to society. Without adequate ethical oversight, cybersecurity risks being viewed as a field driven solely by technical considerations, without regard for the broader implications of its practices. Strengthening ethical oversight is therefore critical to advancing cybersecurity as a mature and respected profession (Baase, 2017).

4.7.4 Rapid Technological Change

4.7.4.1 Description: Rapid technological change in cybersecurity refers to the swift and continuous evolution of digital technologies, including new software, hardware, and methodologies, which significantly impact the field. These changes are driven by innovations in areas such as artificial intelligence, cloud computing, and the Internet of Things (IoT), as well as the increasing sophistication of cyber threats. The pace of technological advancement means that cybersecurity professionals must constantly update their knowledge and skills to keep pace with emerging tools and techniques, as well as evolving threat landscapes.

4.7.4.2 Importance: The importance of rapid technological change in cybersecurity lies in its dual role as both an opportunity and a challenge. On one hand, advancements in technology provide cybersecurity professionals with more powerful tools to protect information systems and data. On the other hand, these changes also introduce new

vulnerabilities and complexities that must be addressed. The speed at which technology evolves can outpace the ability of professionals to adapt, leading to potential gaps in security measures. Additionally, organisations must continuously invest in training and upgrading their cybersecurity infrastructure to stay ahead of these changes, which can be resource-intensive.

4.7.4.3 Implication for Professionalisation: Rapid technological change has profound implications for the professionalisation of the cybersecurity field. To maintain the credibility and relevance of the profession, there must be a strong emphasis on continuous education and professional development. Professional bodies and educational institutions need to regularly update curricula and certification requirements to reflect the latest technological advancements and emerging threats. This ongoing adaptation helps ensure that cybersecurity remains a dynamic and responsive profession, capable of addressing the challenges posed by a rapidly changing digital landscape. Moreover, the ability to manage and adapt to technological change is a hallmark of a mature profession, further solidifying cybersecurity's status as a critical and respected field (Böhme & Moore, 2012).

4.7.5 Fragmentation of Body of Knowledge in Cybersecurity

4.7.5.1 Description: Fragmentation of the body of knowledge in cybersecurity refers to the existence of multiple, often inconsistent or overlapping, sets of knowledge, practices, and standards within the field. This fragmentation can arise from the rapid evolution of cybersecurity threats, the diversity of specialisations within the field, and the varying approaches taken by different organisations, industries, and educational institutions. As a result, there is no single, universally accepted body of knowledge that

encompasses all aspects of cybersecurity, leading to challenges in standardising education, training, and professional practices.

4.7.5.2 Importance: The fragmentation of the body of knowledge in cybersecurity is a significant concern because it hampers the development of a cohesive and unified approach to cybersecurity education and practice. Without a consistent knowledge base, there can be discrepancies in the skills and competencies of cybersecurity professionals, leading to gaps in their ability to address emerging threats effectively. This fragmentation also complicates the creation of standardised certification and accreditation processes, as different organisations may have different criteria for what constitutes essential knowledge and skills. Furthermore, it can lead to inefficiencies and misunderstandings in collaborative efforts, as professionals may lack a common framework for addressing cybersecurity challenges.

4.7.5.3 Implication for Professionalisation: The fragmentation of the body of knowledge in cybersecurity poses a major obstacle to the professionalisation of the field. Professionalisation typically requires a well-defined and standardised body of knowledge that is universally recognised and accepted by practitioners, educators, and employers. The current fragmentation undermines efforts to establish such a foundation, making it difficult to develop consistent educational programmes, certifications, and professional standards. This lack of standardisation can diminish the credibility of the cybersecurity profession and create barriers to the recognition of cybersecurity as a fully-fledged profession. Addressing this fragmentation is crucial for advancing the professionalisation of cybersecurity, as it would enable the establishment of a unified knowledge base that supports the development of a coherent and respected professional community (Von Solms & Van Niekerk, 2013).

4.7.6 Cost and Accessibility of Certifications in Cybersecurity

4.7.6.1 Description: The cost and accessibility of certifications in cybersecurity refer to the financial and logistical barriers that professionals may face when attempting to obtain recognised credentials in the field. Certifications such as CISSP, CEH, CompTIA Security+ and SANS training courses are widely regarded as essential qualifications for advancing in cybersecurity careers. However, the costs associated with these certifications, including exam fees, study materials, and preparatory courses, can be substantial. Accessibility also encompasses the availability of certification exams and training resources, which may be limited by geographical location or language barriers, further challenging individuals in underrepresented regions or communities.

4.7.6.2 Importance: The cost and accessibility of cybersecurity certifications are critical factors that influence the development of a skilled and diverse workforce. High costs can be prohibitive, particularly for early-career professionals or those from lower-income backgrounds, potentially limiting the pool of qualified individuals entering the field. This financial barrier can also exacerbate existing inequalities, preventing capable professionals from disadvantaged regions or communities from accessing the credentials needed to advance their careers. Furthermore, limited accessibility to certification resources and exams can slow the growth of the cybersecurity workforce, which is already facing significant shortages globally. Ensuring that certifications are both affordable and accessible is essential for building a robust, inclusive cybersecurity profession capable of meeting the demands of an increasingly digital world.

4.7.6.3 Implication for Professionalisation: The issues of cost and accessibility in obtaining cybersecurity certifications have significant implications for the professionalisation of the field. Professionalisation requires that a broad and diverse

range of individuals have the opportunity to obtain the necessary qualifications to enter and progress within the profession. If certifications are prohibitively expensive or difficult to access, the field risks becoming exclusive, limiting the diversity of perspectives and skills that are critical for addressing complex cybersecurity challenges. Lowering the cost and increasing the accessibility of certifications would support the development of a more inclusive and equitable profession, helping to ensure that cybersecurity expertise is not concentrated in wealthier regions or among those with greater financial resources. This inclusivity is essential for the long-term sustainability and credibility of the cybersecurity profession, as it seeks to protect a global digital ecosystem (Wilson & Hash, 2003).

4.7.7 Unified Body of Knowledge in Cybersecurity

4.7.7.1 Description: A unified body of knowledge (BoK) in cybersecurity refers to a comprehensive, standardised compilation of the concepts, skills, practices, and frameworks that are essential for professionals in the field. This BoK serves as a foundational reference that guides the education, certification, and professional development of cybersecurity practitioners. It includes a wide range of topics, such as network security, cryptography, risk management, ethical hacking, and legal aspects of cybersecurity. The unified BoK is designed to ensure that all cybersecurity professionals share a common understanding of the core principles and practices that are necessary to protect digital assets and infrastructure effectively.

4.7.7.2 Importance: The importance of a unified body of knowledge in cybersecurity lies in its ability to create consistency and standardisation across the profession. By providing a common framework, the BoK helps to ensure that cybersecurity professionals are equipped with the same foundational knowledge, regardless of their

geographical location or specific area of focus. This standardisation is crucial for the development of educational programmes, certifications, and professional standards, as it ensures that all practitioners meet a recognised baseline of competence. Additionally, a unified BoK facilitates better communication and collaboration among professionals, as it provides a shared language and understanding of key concepts and practices.

4.7.7.3 Implication for Professionalisation: The establishment of a unified body of knowledge is a critical step in the professionalisation of cybersecurity. It helps to formalise the field by defining the scope and content of the knowledge that all professionals in the field should possess. This, in turn, supports the development of consistent and rigorous certification and accreditation processes, which are essential for the recognition of cybersecurity as a legitimate and respected profession. Moreover, a unified BoK enhances the credibility of the cybersecurity profession by ensuring that practitioners are well-prepared to address the complex and evolving challenges of the digital landscape. As cybersecurity continues to grow in importance, the existence of a unified BoK will be key to maintaining high standards and ensuring the ongoing development of the field (ISC2, 2024).

4.8 New Factors Identified

In developing a professionalisation framework for cybersecurity, several new factors have been identified that are critical for addressing the unique challenges of this rapidly evolving field.

These factors, identified through the analysis of existing professionalisation frameworks, are crucial for building a robust, adaptable, and globally recognised cybersecurity profession. Below is a proposed professionalisation framework for cybersecurity. Incorporating these factors into the framework can foster a more holistic approach to developing well-

rounded, skilled, and ethically responsible professionals who are capable of addressing the evolving demands of the field. These factors include:

4.8.1 Cross-Disciplinary Collaboration:

In the field of cybersecurity, cross-disciplinary collaboration is becoming increasingly important. Cybersecurity intersects with multiple fields, including law, psychology, business, and ethics. The ability of cybersecurity professionals to work across these disciplines enhances the development of more comprehensive solutions to complex cyber threats (D'Arcy & Hovav, 2007; Jang-Jaccard & Nepal, 2014).

To strengthen the cybersecurity profession, frameworks should encourage and integrate cross-disciplinary skills, fostering collaboration between technical cybersecurity experts and professionals from law, ethics, psychology, and business (Pfleeger & Cunningham, 2010). Including this factor in the framework could enhance the adaptability and relevance of cybersecurity professionals, ensuring they are equipped to handle the multifaceted nature of modern cyber threats (Von Solms & Van Niekerk, 2013).

4.8.1.1 Legal Collaboration: Collaborating with legal professionals helps ensure that cybersecurity strategies are compliant with national and international laws, such as data protection regulations (e.g., GDPR) (Kuner et al., 2020).

4.8.1.2 Psychological and Behavioral Insights: Cybersecurity must align with business objectives, ensuring that security measures support organisational goals while minimising risks (Ransbotham & Mitra, 2009).

4.8.1.3 Business Strategy: Cybersecurity must align with business objectives, ensuring that security measures support organisational goals while minimising risks.

4.8.1.4 Ethics: Working with ethicists helps professionals navigate the ethical challenges posed by technologies like artificial intelligence, surveillance, and data privacy (Floridi & Taddeo, 2016).

4.8.2 Diversity and Inclusion in Cybersecurity

4.8.2.1 Description: Promoting diversity and inclusion within the cybersecurity workforce can lead to a more creative and adaptive approach to tackling cyber threats (World Economic Forum, 2020; ISACA, 2020b). A diverse team brings different perspectives, problem-solving approaches, and experiences, which can improve both the resilience and innovation of security solutions (Ashenden & Lawrence, 2016).

4.8.2.2 Importance: Encouraging underrepresented groups to pursue careers in cybersecurity and creating an inclusive working environment can fill the talent gap and foster a broader range of insights and solutions.

4.8.2.3 Implication for Professionalisation: Developing mentorship programs, scholarships, and inclusive hiring practices as part of the professionalisation framework can help improve diversity and address workforce shortages (ISC2, 2019).

4.8.3 Cybersecurity Ethics Education

4.8.3.1 Description: As cybersecurity threats evolve, so do ethical dilemmas involving data privacy, AI surveillance, and the balance between security and individual rights (Loi & Christen, 2019). Ethical decision-making must become a core competency for cybersecurity professionals.

4.8.3.2 Importance: The rapid integration of technologies like artificial intelligence, machine learning, and big data in cybersecurity creates significant ethical challenges that need to be addressed (Taddeo, 2017). Professionals must be equipped with the ability to navigate these ethical complexities (Brey, 2012).

4.8.3.3 Implication for Professionalisation: Integrating formal ethical education into certification and training programs can help professionals develop the ability to make ethically sound decisions in complex, real-world situations (Umbrello, 2017).

4.8.4 Soft Skills and Communication

4.8.4.1 Description: While cybersecurity is often seen as a technical field, professionals increasingly need strong soft skills, particularly communication, to explain complex issues to non-technical stakeholders, negotiate with partners, and collaborate across teams (Paulsen et al, 2012).

4.8.4.2 Importance: Cybersecurity professionals must effectively communicate risks, strategies, and compliance needs to a broad audience, including executives, legal teams, and customers (Ashenden & Sasse, 2013).

4.8.4.3 Implication for Professionalisation: Soft skills training, such as public speaking, negotiation, and collaboration, should be incorporated into the cybersecurity professionalisation framework to ensure well-rounded professionals who can effectively advocate for security measures (Schein, 2017).

4.8.5 Lifelong Learning and Adaptability

4.8.5.1 Description: Given the dynamic nature of cybersecurity, professionals must commit to lifelong learning to stay updated on emerging threats, technologies, and regulations (Bada & Sasse, 2014).

4.8.5.2 Importance: The rapidly changing landscape of cybersecurity necessitates that professionals constantly upgrade their knowledge and skills. This requires a mindset of continuous adaptation (Von Solms & Van Niekerk, 2013).

4.8.5.3 Implication for Professionalisation: Building an environment that encourages ongoing learning through micro-credentials, modular certifications, and

continual professional development ensures that cybersecurity professionals are equipped to handle new challenges (ISC2, 2023).

4.8.6 Resilience Engineering

4.8.6.1 Description: Resilience engineering focuses on preparing systems and organisations to withstand and recover from cyberattacks (Woods & Hollnagel, 2017). This concept shifts focus from simply preventing attacks to ensuring that systems can quickly recover and maintain operations during disruptions.

4.8.6.2 Importance: As cyberattacks become more sophisticated, it is no longer enough to prevent breaches; organisations need professionals trained to design systems that are resilient and recoverable.

4.8.6.3 Implication for Professionalisation: Integrating resilience engineering into professional certifications and education programs will equip cybersecurity professionals to build more robust systems and mitigate the effects of inevitable cyberattacks (Linkov et al., 2013).

4.8.7 Professional Licensing

4.8.7.1 Description: Professional licensing in cybersecurity involves the certification of individuals who have demonstrated proficiency in specific competencies, ethical standards, and technical knowledge required to protect digital infrastructures. Licensing often requires completing accredited educational programmes, passing rigorous examinations, and adhering to a code of ethics. This process ensures that licensed professionals meet a recognised standard of practice that is consistent across the industry.

4.8.7.2 Importance: The importance of professional licensing in cybersecurity is significant as it establishes a benchmark for the skills and knowledge necessary to

perform in the field. As cyber threats become increasingly sophisticated, ensuring that professionals possess the requisite expertise is crucial to safeguarding sensitive information and critical systems. Licensing also helps to protect the public by ensuring that only qualified individuals are allowed to perform high-stakes cybersecurity tasks, reducing the risk of breaches and data loss.

4.8.7.3 Implication for Professionalisation: The implementation of professional licensing has profound implications for the professionalisation of the cybersecurity field. Licensing formalises the profession by creating clear entry requirements and career advancement pathways, which are essential components of any recognised profession. This formalisation supports the development of a standardised body of knowledge, encourages ongoing education and professional development, and enhances the public's trust in the field. Moreover, it facilitates regulatory oversight and accountability, contributing to the overall stability and maturity of the cybersecurity profession. According to the National Initiative for Cybersecurity Education (NICE) framework, such formalised structures are pivotal in developing a well-defined cybersecurity workforce and advancing the professionalisation of the industry (Newhouse et al., 2017).

4.8.8 Practice Insurance

4.8.8.1 Description: Practice insurance, also known as professional liability insurance or errors and omissions insurance, is a type of coverage designed to protect cybersecurity professionals from potential legal claims and financial losses resulting from errors, omissions, or negligence in the performance of their professional duties. This insurance provides a safety net for professionals, covering the costs of legal defense, settlements, and judgments that may arise from allegations of failure to deliver

services as promised or from unintended mistakes that lead to data breaches or other security incidents.

4.8.8.2 Importance: The importance of practice insurance in cybersecurity is paramount, given the high stakes involved in the protection of sensitive data and critical infrastructure. As cybersecurity professionals are increasingly held liable for the security of their clients' digital assets, practice insurance becomes a critical component of risk management. It not only protects individual practitioners and firms from potentially devastating financial consequences but also reinforces trust with clients who are assured that any potential mishaps will be handled professionally and without undue financial strain on the service provider.

4.8.8.3 Implication for Professionalisation: The adoption of practice insurance has significant implications for the professionalisation of the cybersecurity field. It underscores the recognition of cybersecurity as a mature profession, where practitioners are expected to manage and mitigate the risks associated with their work. By institutionalising the requirement for practice insurance, the field establishes a standard of accountability and responsibility, which are hallmarks of professional practice. Furthermore, it encourages cybersecurity professionals to adhere to best practices, continuously update their skills, and maintain high ethical standards, knowing that their practice insurance is contingent upon these factors. This alignment with broader professional norms helps to elevate the status of cybersecurity as a fully professionalised field, akin to established professions such as law and medicine (National Research Council, 2013; ISACA, 2020a).

4.8.9 Cybersecurity Bills

4.8.9.1 Description: Cybersecurity bills refer to legislative measures enacted by governments to regulate and secure various aspects of digital infrastructure, data protection, and cyber incident management. These laws establish legal frameworks for the protection of critical infrastructure, mandate the reporting of significant cyber incidents, and outline the responsibilities of both public and private entities in safeguarding digital assets. Notable examples include the General Data Protection Regulation (GDPR) in Europe, the Network and Information Systems (NIS) Directive in the United Kingdom, and the Computer Misuse and Cybersecurity Bills in Singapore.

4.8.9.2 Importance: The importance of cybersecurity bills is underscored by their role in creating a robust legal foundation for national and economic security in an increasingly digital world. These bills provide clear guidelines and standards that organisations must adhere to, ensuring a consistent approach to cybersecurity across industries. By mandating best practices and incident reporting, these laws enhance the overall resilience of digital infrastructures against cyber threats. Additionally, cybersecurity bills facilitate cooperation between government agencies and the private sector, fostering a more unified and effective defence against cyber-attacks.

4.8.9.3 Implication for Professionalisation: The implementation of cybersecurity bills has profound implications for the professionalisation of the cybersecurity field. These laws compel organisations to seek out highly qualified cybersecurity professionals who are capable of ensuring the compliance with complex legal requirements. As cybersecurity legislation becomes more intricate, the demand for professionals with both technical expertise and a thorough understanding of legal frameworks will grow. Furthermore, the recognition of cybersecurity within the legal domain reinforces its status as a specialised profession, comparable to established fields

such as law and healthcare. This legal recognition promotes the development of tailored educational programmes, certifications, and professional standards, thereby advancing the formalisation and professionalisation of cybersecurity (Deibert, 2012).

4.8.10 Job Roles and Career Pathways

4.8.10.1 Description: Job roles and career pathways in cybersecurity refer to the structured progression of positions and professional opportunities available within the field. These pathways often begin with entry-level roles, such as security analysts or incident responders, and can advance to more specialised positions, such as penetration testers, cybersecurity architects, or chief information security officers (CISOs). Career pathways are typically supported by a combination of formal education, certifications, and practical experience, allowing professionals to advance in their careers by acquiring new skills and taking on more complex responsibilities.

4.8.10.2 Importance: The importance of clearly defined job roles and career pathways in cybersecurity lies in their ability to provide structure and direction for professionals entering the field. Well-defined roles help organisations identify and recruit the right talent, ensuring that individuals with the appropriate skills are matched to the tasks and responsibilities required by the position. Career pathways, on the other hand, offer a roadmap for professional growth, encouraging continuous learning and skill development. This not only benefits individual professionals by providing them with opportunities for advancement but also strengthens the overall cybersecurity workforce by ensuring a pipeline of skilled practitioners who are prepared to meet the evolving challenges of the field.

4.8.10.3 Implication for Professionalisation: The establishment of job roles and career pathways has significant implications for the professionalisation of the

cybersecurity field. By delineating clear roles and progression routes, the field is formalised, akin to other established professions such as law or medicine. This formalisation supports the development of standardised educational and certification programmes, which are essential for ensuring that professionals have the competencies required for specific roles. Additionally, well-defined career pathways contribute to the recognition of cybersecurity as a distinct and credible profession, attracting talent and fostering a sense of professional identity among practitioners. As the field continues to mature, these pathways will likely play a critical role in shaping the future of cybersecurity, ensuring that it remains responsive to the needs of both the industry and society (Pfleeger & Cunningham, 2019).

4.8.11 Code of Conduct

4.8.11.1 Description: A code of conduct in cybersecurity is a formalised set of ethical guidelines and professional standards that govern the behaviour and decision-making processes of cybersecurity professionals. This code outlines the responsibilities of practitioners to act with integrity, confidentiality, and respect for privacy while protecting digital assets and infrastructure. It serves as a benchmark for acceptable professional behaviour, ensuring that cybersecurity professionals uphold the highest ethical standards in their work.

4.8.11.2 Importance: The importance of a code of conduct in cybersecurity is rooted in its role as a foundational element of professional integrity and trust. Given the sensitive nature of the information and systems that cybersecurity professionals handle, adhering to a strict code of conduct is essential for maintaining public trust and ensuring the responsible management of digital resources. It helps to mitigate risks associated with unethical behaviour, such as data breaches, insider threats, and misuse of privileged

information. Moreover, a code of conduct fosters a culture of accountability and transparency within the profession, guiding practitioners in navigating complex ethical dilemmas that may arise in their work.

4.8.11.3 Implication for Professionalisation: The adoption and enforcement of a code of conduct have significant implications for the professionalisation of the cybersecurity field. By establishing a clear set of ethical guidelines, a code of conduct formalises the expectations for professional behaviour, thereby helping to elevate the status of cybersecurity as a recognised and respected profession. It encourages the development of a shared professional identity among cybersecurity practitioners, who are bound by common ethical standards. Additionally, the existence of a code of conduct supports the development of certification and accreditation programmes, as adherence to ethical standards becomes a criterion for professional recognition. This alignment with broader professional norms helps to ensure that cybersecurity professionals are not only technically competent but also ethically sound, contributing to the overall maturity and legitimacy of the field (Whitman & Mattord, 2018).

4.8.12 Regulatory Framework

4.8.12.1 Description: A regulatory framework in cybersecurity consists of a structured set of laws, guidelines, and standards designed to govern the protection of digital infrastructures, data privacy, and the management of cyber risks. These frameworks are established by governments and international bodies to ensure that organisations adhere to best practices in cybersecurity, mitigate the impact of cyber threats, and protect the integrity of critical systems and sensitive information. Notable examples of such frameworks include the General Data Protection Regulation (GDPR) in Europe, the Health Insurance Portability and Accountability Act (HIPAA) in the

United States, which governs the protection of healthcare information, the Sarbanes-Oxley Act (SOX), which sets requirements for financial record-keeping and reporting in public companies, and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), which provides a voluntary framework for improving cybersecurity practices across industries.

4.8.12.2 Importance: The importance of a regulatory framework in cybersecurity lies in its ability to create a consistent and enforceable approach to digital security across industries and borders. By establishing clear requirements and standards, regulatory frameworks ensure that organisations implement adequate security measures to protect against cyber threats, thereby reducing vulnerabilities and enhancing the overall resilience of the digital ecosystem. For instance, HIPAA mandates strict data protection measures for healthcare providers, SOX requires stringent controls over financial information to prevent fraud, and the NIST CSF offers a flexible yet comprehensive set of guidelines that can be adapted to various sectors to bolster their cybersecurity posture. These frameworks also provide a legal basis for penalising non-compliance, which acts as a deterrent against negligence and encourages a proactive approach to cybersecurity. Furthermore, they facilitate international cooperation, enabling countries to align their cybersecurity efforts and respond more effectively to cross-border cyber threats.

4.8.12.3 Implication for Professionalisation: The establishment of regulatory frameworks has significant implications for the professionalisation of the cybersecurity field. These frameworks create a demand for professionals who not only possess technical skills but also have a deep understanding of legal and regulatory requirements. For example, cybersecurity experts working in healthcare must be familiar with HIPAA regulations, those in the financial sector must understand the requirements of SOX, and

professionals across various industries benefit from understanding and applying the NIST CSF. As compliance becomes increasingly complex, cybersecurity professionals must continually update their knowledge and skills to stay abreast of evolving regulations. This demand drives the development of specialised training programmes and certifications, which are essential for the formalisation of cybersecurity as a recognised profession. Moreover, the existence of a regulatory framework elevates the accountability and responsibility of cybersecurity professionals, aligning the field with other established professions where adherence to regulatory standards is a core aspect of practice (Greenleaf, 2012).

4.8.13 Technical Skills and Competency Levels

4.8.13.1 Description: Technical skills and competency levels in cybersecurity refer to the specific abilities and knowledge required to effectively protect information systems, networks, and data from cyber threats. These skills include, but are not limited to, understanding network security, cryptography, incident response, ethical hacking, and risk management. Competency levels, often categorised from beginner to expert, reflect the depth of proficiency an individual has in these areas. These levels are typically assessed through certifications, practical experience, and continuous education, ensuring that cybersecurity professionals possess the necessary skills to meet industry demands.

4.8.13.2 Importance: The importance of technical skills and clearly defined competency levels in cybersecurity lies in their critical role in maintaining the security and integrity of digital infrastructures. As cyber threats become more sophisticated, it is essential that cybersecurity professionals are equipped with up-to-date technical skills to effectively counter these threats. Competency levels serve as a benchmark for

evaluating the abilities of professionals, ensuring that they are adequately prepared to handle the complexities of their roles. This not only enhances the effectiveness of cybersecurity measures within organisations but also contributes to the overall resilience of the digital economy.

4.8.13.3 Implication for Professionalisation: The emphasis on technical skills and competency levels has significant implications for the professionalisation of the cybersecurity field. By establishing clear standards for what constitutes proficiency at various levels, the field becomes more structured and formalised. This formalisation supports the development of standardised training and certification programmes, which are essential for ensuring consistency and quality across the profession. Furthermore, the recognition of different competency levels encourages continuous professional development, as practitioners are motivated to advance their skills and move up the competency ladder. This progression contributes to the growth of a well-defined professional community, where members are recognised not only for their experience but also for their specialised expertise. As the field continues to evolve, the focus on technical skills and competency levels will play a pivotal role in shaping the standards and expectations of the cybersecurity profession (National Initiative for Cybersecurity Education, 2020; ISACA, 2021).

4.8.14 Unified Body of Knowledge

4.8.14.1 Description: A unified body of knowledge in cybersecurity refers to a comprehensive and standardised collection of concepts, principles, methodologies, and best practices that define the essential knowledge required for the profession. This body of knowledge encompasses a wide range of topics, including network security, cryptography, risk management, ethical hacking, and compliance with legal and

regulatory frameworks. It serves as the foundational knowledge base that guides the education, training, and certification of cybersecurity professionals, ensuring consistency and coherence across the field.

4.8.14.2 Importance: The importance of a unified body of knowledge in cybersecurity lies in its ability to standardise the education and practice of cybersecurity professionals globally. By defining what professionals need to know and understand, this unified body of knowledge ensures that there is a common understanding of key concepts and practices across the industry. This standardisation is crucial for developing curricula for academic programmes, creating certification exams, and guiding professional development initiatives. It also facilitates collaboration and communication among professionals, as they share a common language and framework for discussing cybersecurity issues and solutions.

4.8.14.3 Implication for Professionalisation: The development and adoption of a unified body of knowledge have profound implications for the professionalisation of the cybersecurity field. By establishing a recognised and standardised knowledge base, the field takes a significant step towards formalising the profession, similar to how law and medicine have well-defined bodies of knowledge. This formalisation supports the creation of uniform certification standards and accreditation processes, which are essential for ensuring that professionals across the globe meet consistent and high standards of practice. Moreover, a unified body of knowledge reinforces the identity of cybersecurity as a distinct and credible profession, attracting new talent and providing a clear pathway for career advancement. As the cybersecurity landscape continues to evolve, the maintenance and updating of this unified body of knowledge will be critical

to keeping the profession relevant and effective in addressing emerging threats (Whitman & Mattord, 2018).

4.8.15 Adoption and Translation of Body of Knowledge

4.8.15.1 Description: The adoption and translation of a body of knowledge in cybersecurity involve the process of integrating and applying a standardised set of concepts, practices, and principles across different contexts, industries, and regions. Adoption refers to the acceptance and utilisation of a unified body of knowledge by educational institutions, certification bodies, and professional organisations. Translation, on the other hand, involves adapting this body of knowledge to meet the specific needs and challenges of various sectors and geographical areas, ensuring that the knowledge remains relevant and practical in diverse environments.

4.8.15.2 Importance: The adoption and translation of a unified body of knowledge in cybersecurity are crucial for creating a consistent and coherent foundation for the education and training of professionals across the globe. By adopting a standardised body of knowledge, institutions and organisations can ensure that cybersecurity professionals possess the necessary skills and understanding to address global cyber threats effectively. Translation of this knowledge into different contexts ensures that it is applicable and relevant, taking into account local regulations, industry-specific requirements, and cultural differences. This dual process of adoption and translation helps bridge gaps between global standards and local practices, ensuring that cybersecurity measures are both comprehensive and adaptable.

4.8.15.3 Implication for Professionalisation: The successful adoption and translation of a unified body of knowledge have significant implications for the professionalisation of cybersecurity. By embracing a common set of standards and practices, the field can

move towards greater formalisation, akin to other established professions such as engineering or medicine. This process supports the development of globally recognised certifications and educational programmes, which are essential for ensuring that cybersecurity professionals meet high standards of competence and ethics, regardless of where they practice. Moreover, the ability to translate and adapt this knowledge to different contexts enhances the profession's flexibility and responsiveness to new challenges, reinforcing its credibility and relevance in a rapidly changing technological landscape (Craigen et al., 2014).

4.8.16 Professional Associations' Role in Professionalisation

4.8.16.1 Description: Professional associations are organisations that represent the interests of individuals within a specific profession. In cybersecurity, these associations play a pivotal role in the professionalisation of the field by establishing standards, advocating for the profession, providing certifications, and fostering a sense of community among practitioners. These associations often set the ethical guidelines, offer continuing education opportunities, and support the development of a unified body of knowledge, which is essential for the formal recognition of cybersecurity as a distinct profession.

4.8.16.2 Importance: The importance of professional associations in cybersecurity lies in their ability to provide structure and legitimacy to the field. They serve as gatekeepers for professional standards by ensuring that members adhere to established ethical practices and meet the necessary competencies. Professional associations also contribute to the credibility of the profession by offering certifications that validate the skills and knowledge of practitioners. Furthermore, they provide networking

opportunities, allowing professionals to share knowledge, stay updated with industry trends, and collaborate on initiatives that advance the field.

4.8.16.3 Implication for Professionalisation: The involvement of professional associations is crucial for the ongoing professionalisation of cybersecurity. By establishing and maintaining standards, these associations help to formalise the profession, making it more recognisable and respected. Their role in certification and continuing education ensures that practitioners are competent and committed to lifelong learning, which is essential in a field as dynamic as cybersecurity. Additionally, professional associations advocate for the interests of the profession at policy levels, influencing regulations and standards that shape the industry. This advocacy helps to position cybersecurity as a vital and mature profession, aligning it with other established fields such as law or medicine (Von Solms & Van Niekerk, 2013).

4.8.17 Sustainable Development

4.8.17.1 Description: Sustainable development in cybersecurity refers to the integration of sustainability principles into cybersecurity practices, policies, and strategies. This involves considering the long-term impact of cybersecurity measures on the environment, society, and economy. Sustainable cybersecurity practices might include energy-efficient data centres, reducing the carbon footprint of digital infrastructure, ensuring equitable access to cybersecurity resources, and promoting responsible consumption of digital services. The goal is to develop and implement cybersecurity solutions that protect digital assets while also contributing to broader sustainability goals.

4.8.17.2 Importance: The importance of sustainable development in cybersecurity is becoming increasingly recognised as digitalisation continues to grow globally. As the

reliance on digital infrastructure expands, so does the environmental impact, particularly in terms of energy consumption and e-waste. By integrating sustainability into cybersecurity, organisations can reduce their environmental footprint and contribute to global efforts to combat climate change. Additionally, sustainable practices can enhance social equity by ensuring that cybersecurity resources and protections are accessible to all, particularly in underserved communities. This approach not only helps in mitigating environmental risks but also promotes social responsibility and economic stability.

4.8.17.3 Implication for Professionalisation: The incorporation of sustainable development into cybersecurity has significant implications for the professionalisation of the field. As sustainability becomes a key consideration in business and policy decisions, cybersecurity professionals will need to develop new competencies and knowledge areas related to sustainable practices. This shift will likely lead to the emergence of new standards and certifications that reflect the importance of sustainability in cybersecurity. Furthermore, by aligning with sustainability goals, the cybersecurity profession can enhance its credibility and relevance in the global context, demonstrating a commitment to not only protecting digital assets but also contributing positively to the environment and society (GeSI, 2016).

4.9 Synthesis of Findings

The meta-analysis revealed several important patterns across different professions that can inform the professionalisation of cybersecurity. Success factors such as standardised certification, ethical oversight, continuous professional development, and global standardisation are essential components of a strong professionalisation framework. These elements contribute to the credibility and recognition of professionals in established fields and should be central to the design of a cybersecurity professionalisation framework.

At the same time, challenges such as fragmented certification systems, resistance to standardisation, and the lack of ethical oversight highlight the potential obstacles that cybersecurity must overcome to achieve a cohesive and globally recognised profession. Addressing these challenges will require collaboration between governments, industry leaders, and professional bodies to create a unified, standardised approach to cybersecurity professionalisation.

In addition, several new factors are crucial for developing a robust cybersecurity profession. Cross-disciplinary collaboration, diversity and inclusion, and strong soft skills and communication are vital for addressing complex, multifaceted challenges. A focus on lifelong learning, resilience engineering, and clear career pathways ensures professionals remain adaptable in a rapidly evolving field.

Key structural elements also include professional licensing, practice insurance, and cybersecurity legislation to establish legal and regulatory standards. A unified body of knowledge, along with professional associations advocating for standards and certifications, will create a cohesive, globally recognised profession that is prepared for sustainable growth. With these, a new proposed professionalisation (see Figure 9) is proposed:

Figure 9

Proposed Professionalisation Framework

4.10 Summary

The results of this meta-analysis provide a clear understanding of the key success factors and challenges involved in the professionalisation of various professions. These insights are critical for informing the development of a professionalisation framework for cybersecurity, which must incorporate standardised certification, strong ethical guidelines, continuous professional development, and global standardisation.

By addressing the challenges of fragmentation, resistance to standardisation, and rapid technological change, the cybersecurity profession can evolve into a globally recognised and trusted field (National Research Council, 2013).

Chapter 5. Discussion

5.0 Discussion of the study

This study undertook a comprehensive meta-analysis of professionalisation frameworks across multiple professions, aiming to identify the factors contributing to their success or failure and to apply these insights to the field of cybersecurity. The professions studied—medicine, law, engineering, education, and information technology - each offer unique perspectives on the process of professionalisation.

The findings highlighted that successful professionalisation frameworks share common elements such as rigorous certification processes, adherence to ethical guidelines, mandatory continuous professional development, and the presence of strong governing bodies. These elements have enabled these professions to maintain high standards of practice, adapt to evolving challenges, and earn the trust of the public.

In contrast, professions that have struggled to establish effective professionalisation frameworks, such as education and early-stage IT, often lacked standardisation, cohesive governance, and consistent enforcement of ethical practices. These failures have resulted in fragmented practices, varying levels of professional recognition, and challenges in maintaining the credibility and effectiveness of practitioners. The cybersecurity profession, which currently faces similar challenges, can learn valuable lessons from these successes and failures as it seeks to develop its own framework.

5.1 Limitations and Strengths

This study, while comprehensive in its scope, is not without its limitations. One significant limitation is the reliance on existing literature and secondary data for the meta-analysis. This approach, while valuable for synthesising a wide range of findings, may not capture the most current developments in rapidly evolving fields such as cybersecurity.

Additionally, the study's focus on well-established professions may have led to the exclusion of insights from emerging or less formalised fields that could offer innovative approaches to professionalisation. Another limitation is the potential for bias in the selection of professions and frameworks analysed, as the study may have prioritised those with more readily available or documented success stories.

Despite these limitations, the study has several notable strengths. The comparative analysis across multiple, diverse professions provides a broad perspective on the factors that contribute to successful professionalisation. This cross-disciplinary approach allows for the identification of universal principles that can be applied to the unique challenges of cybersecurity. Furthermore, the study's focus on both successes and challenges offers a balanced view, highlighting not only what works but also the pitfalls to avoid. These strengths ensure that the findings are robust and can be effectively applied to guide the development of a more cohesive and effective professionalisation framework for the cybersecurity profession.

5.2 Implications of Cybersecurity Education and Training

The insights gained from this study have significant implications and impacts for the professionalisation of cybersecurity. Given the current global settings and rapidly evolving nature of the cyber threats landscape, it is imperatively important that the cybersecurity profession adopts a solid and robust trusted framework that will incorporate those critical success factors identified in this study.

This includes the establishment of a globally recognised certification process, the enforcement of ethical guidelines and education tailored to the unique challenges of cybersecurity. In addition, the necessity to integrate the mandatory continuous professional development requirements to ensure that practitioners remain up-to-date with the latest threats and technologies.

Furthermore, the development of a strong governing body or consortium of bodies is crucial to overseeing the implementation and maintenance of this framework. Such an organisation would be responsible for standardising certification requirements, enforcing ethical standards, and promoting continuous learning within the profession. By adopting these elements, the cybersecurity profession can enhance its credibility, attract more qualified individuals, and better protect global digital infrastructure.

5.3 Implications of Mutual Recognition Agreements

For cybersecurity professionalisation, the Mutual Recognition Agreements (MRAs) play an important role as it ensures that the long-term success of the implementation of framework. It also facilitates cross-border work in different countries and regions, seeking recognition of qualifications, skills, and professional standards among the participating countries. This enables the cybersecurity workforce to be globally work-ready and able to navigate more efficiently and effectively in a diverse and regulated landscapes across countries and regions. It also fosters consistency and increases trust in professional capabilities as part of the modern work force to increase mobility.

Together with CPD that ensures the cybersecurity professionals continually updating their knowledge and skills, it allows them to keep pace with the rapid technological changes and accustomed to the needs of the requirements of CPD. These elements enhance the sustainability of the profession by promoting both international mobility and lifelong learning, which are crucial for adapting to new challenges and maintaining a high level of competency.

5.4 Recommendations

While this study provides a solid foundation for understanding the elements of successful professionalisation frameworks, further studies are needed to refine and adapt these

insights specifically for cybersecurity. Future research could explore the development of a competency-based framework tailored to different specialisations within cybersecurity.

These may include topics such as offensive security, secure coding, operational technology cybersecurity (CSA, 2019), or user and entity behaviour analytics, etc. In addition, further studies may include the investigation of emerging technologies, such as artificial intelligence and machine learning, development security operations (DevSecOps), quantum security, in shaping the future of cybersecurity professionalisation with the knowledge of emerging technologies.

Another area for future research is the exploration of regional variations in cybersecurity threats and practices, and how these might influence the development of localised professionalisation frameworks that still align with global standards. Finally, longitudinal studies that track the effectiveness of newly implemented frameworks in cybersecurity over time would provide valuable data to further refine and improve these frameworks.

5.5 Concluding the Study

The process of professionalisation is important and critical for establishing the credibility, trust, and effectiveness of any profession. As the cybersecurity field continues to grow in importance, it must adopt a holistic, comprehensive and cohesive professionalisation framework that addresses the unique challenges it faces (BCS, 2015).

By drawing insights from the successes and challenges of other professions covered in this study, a more complete and holistic cybersecurity framework can be developed based on these identified factors. Such a framework would help in upholding high standards for professional practice but also encourage a culture of continuous and ongoing learning, ethical responsibility, and innovation in this profession.

In addition, the study identified new opportunities for collaboration between industry, academia, and government agencies. These new elements will help to strengthen the quality of the cybersecurity workforce and their competence level by aligning technical training and education with the real-world needs and demands. These partnerships would definitely create avenues for better training programmes, with real-life practical experience, and improved career pathway and opportunities. This approach will further enhance the readiness of cybersecurity professionals that is more ready for the ever-evolving cyber security landscape.

This proposed new framework would better equip cybersecurity professionals to protect the critical infrastructure in the digital landscape, stay ahead of the emerging cybersecurity threats and mitigate any potential risks. This helps to maintain the trust of individuals and organisations that depend on their expertise and for the betterment of the organisations' security posture. Furthermore, the fostering of innovation and cross-sector collaboration will help to shape the adaptive security strategies, ensuring cybersecurity professionals can proactively address future challenges.

References

References marked with an asterisk indicate studies included in the meta-analysis.

Andersson, D., & Reimers, K. (2009). CIS and information technology certifications: Education program trends and implications. *Journal of Educational Technology*, *6*(3), 34–41. https://doi.org/10.26634/jet.6.3.1061

*Andrade-Arenas, L., Llulluy-Nuñez, D., Vilchez-Sandoval, J., Carmen, H. R.-D., Romero-Untiveros, L., Lara-Herrera, J., & Alata-Palacios, J. (2023). Innovative proposed model between formative research and accreditation of engineering programs. *International Journal of Engineering Pedagogy*, *13*(4), 113–140. https://doi.org/10.3991/ijep.v13i4.37149 *

Ashenden, D., & Lawrence, D. (2016). Security dialogues: Building better relationships between security and business. *IEEE Security & Privacy, 14*(3), 82-87. https://doi.org/10.1109/MSP.2016.56

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy. *Computers & Security*, *39*, 396-405. https://doi.org/10.1016/j.cose.2013.09.004

Association of Information Security Professionals (AiSP). (2022). *IS-BOK 2.0: Information security body of knowledge V2.0*. https://www.aisp.sg/bok.html/

AustCyber. (2018). *Australian cyber security skills framework*. https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/cyber-skills-framework

Baase, S. (2017). *A gift of fire: Social, legal, and ethical issues for computing technology* (5th ed.). Pearson. https://dl.acm.org/doi/10.5555/3153656

Bada, M., & Sasse, A. M. (2014). Cyber security awareness campaigns: Why do they fail to change behaviour? *Global Cyber Security Capacity Centre*.

https://www.researchgate.net/publication/336676387_Cyber_Security_Awareness_Campaigns_Why_do_they_fail_to_change_behaviour

BCS. (2015). *BCS and the professionalisation of the cyber security industry*. BCS. https://www.bcs.org/articles-opinion-and-research

Bendler, D., & Felderer, M. (2023). Competency models for information security and cybersecurity professionals: Analysis of existing work and a new model. *ACM Transactions on Computing Education*, *23*(2). https://doi.org/10.1145/3573205

Böhme, R., & Kataria, G. (2006). Models and measures for correlation in cyber-insurance. In *Proceedings of the 5th Workshop on the Economics of Information Security* (WEIS 2006). https://core.ac.uk/download/162458449.pdf

Böhme, R., & Moore, T. (2012). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection, 4*(3-4), 136-144. https://doi.org/10.1016/j.ijcip.2011.12.002

Borenstein, M., Hedges, L. V., Higgins, J. P. T., & Rothstein, H. R. (2010). A basic introduction to fixed-effect and random-effects models for meta-analysis. *Research Synthesis Methods, 1*(2), 97-111. https://doi.org/10.1002/jrsm.12

Borenstein, M., Hedges, L. V., Higgins, J. P. T., & Rothstein, H. R. (2009). *Introduction to meta-analysis*. Wiley. https://doi.org/10.1002/9780470743386

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brey, P. (2012). Anticipating ethical issues in emerging IT. *Ethics and Information Technology, 14*(4), 301-316. https://doi.org/10.1007/s10676-012-9293-y

Brockmann, M., Clarke, L., & Winch, C. (2008). Knowledge, skills, competence: European divergences in vocational education and training (VET)—the English, German and

Dutch cases. *Oxford Review of Education, 34*(5), 547-567. https://doi.org/10.1080/03054980701782098

Cameron III, G. D. (2000). Ethics and equity: Enforcing ethical standards in commercial relationships. *Journal of Business Ethics*, *23*(2), 161–172. https://doi.org/10.1023/A:1006025226355

Canadian Centre for Cyber Security. (2020). *Cybersecurity competency framework*. https://www.cyber.gc.ca/en/education-community/academic-outreach-cyber-skills-development/canadian-cyber-security-skills-framework

*Cilia, K. (2023). No quick fix: A sustainable solution to lab personnel shortages. *Medical Laboratory Observer (MLO)*, *55*(6), 1. https://www.mlo-online.com/management/careers/article/53057863/no-quick-fix-a-sustainable-solution-to-lab-personnel-shortages *

Cohen, J. (1988). *Statistical power analysis for the behavioural sciences* (2nd ed.). Lawrence Erlbaum Associates. https://doi.org/10.2307/2290095

Cohen, J. (1992). A power primer. *Psychological Bulletin*, 112(1), 155–159. https://doi.org/10.1037/0033-2909.112.1.155

*Cooklev, T. (2010). The role of standards in engineering education. *International Journal of IT Standards and Standardization Research*, *8*(1), 1. https://doi.org/10.4018/jitsr.2010120701 *

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10), 13-21. https://doi.org/10.22215/timreview/835

Cyber Security Agency of Singapore. (2019). *Singapore operational technology cybersecurity masterplan*. Cyber Security Agency of Singapore.

https://www.csa.gov.sg/News/Publications/singapore-operational-technology-cybersecurity-masterplan

Cybersecurity Body of Knowledge (CyBOK). (2019). *Cybersecurity Body of Knowledge (CyBOK)*. https://www.cybok.org/

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117. https://doi.org/10.1145/1290958.1290971

*Dare, T. (2016). Ethics and the law: An introduction. *Legal Ethics, 19*(1), 182-185. https://doi.org/10.1080/1460728x.2016.1190103. *

Davies, M. (2005). A new training initiative for the lay magistracy in England and Wales—a further step towards professionalisation? *International Journal of the Legal Profession*, *12*(1), 93–119. https://doi.org/10.1080/09695950500081390

Deibert, R. J. (2012). The geopolitics of internet control: Censorship, sovereignty, and cyberspace. *Cambridge Review of International Affairs, 25*(3), 377-397. https://doi.org/10.1080/09557571.2012.710582

Dymock, D., & Tyler, M. (2018). Towards a more systematic approach to continuing professional development in vocational education and training. *Studies in Continuing Education*, *40*(2), 198–211. https://doi.org/10.1080/0158037X.2018.1449102

Ellis, P. D. (2010). *The essential guide to effect sizes: Statistical power, meta-analysis, and the interpretation of research results*. Cambridge University Press. https://doi.org/10.1017/CBO9780511761676

Eraut, M. (1994). *Developing professional knowledge and competence*. Routledge. https://doi.org/10.4324/9780203486016

European Union Agency for Cybersecurity (ENISA). (2022). *European Cybersecurity Skills Framework*. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework

European Union Agency for Cybersecurity. (2017). *Cybersecurity education and training: A key enabler for a cyber-secure Europe*. ENISA. https://www.enisa.europa.eu

Evetts, J. (2013). Professionalism: Value and ideology. *Current Sociology Review, 61*(5-6), 778-796. https://doi.org/10.1177/0011392113479316

*Fanto, J. A. (2021). The professionalization of compliance: Its progress, impediments, and outcomes. *Notre Dame Journal of Law, Ethics & Public Policy*, *35*(1), 183–239. https://doi.org/10.2139/ssrn.3678677 *

Field, A. P., & Gillett, R. (2010). How to do a meta-analysis. *British Journal of Mathematical and Statistical Psychology (2010)*, *63*, 665-694. https://doi.org/10.1348/000711010x502733

*Fleck, L. M. (2020). Medical ethics: A distinctive species of ethics. *Cambridge Quarterly of Healthcare Ethics*, *29*(Issue 3), 421–425. https://doi.org/10.1017/s0963180120000158 *

Floridi, L., & Taddeo, M. (2016). What is data ethics? *Philosophical transactions of the royal society A: Mathematical, Physical and Engineering Sciences, 374*(2083). https://doi.org/10.1098/rsta.2016.0360

*Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers & Security, 109*, Article 102392. https://doi.org/10.1016/j.cose.2021.102392. *

Freidson, E. (2001). Professionalism: The third logic. *University of Chicago Press*. https://www.researchgate.net/publication/37689531_Professionalism_the_third_logic_on_the_practice_of_knowledge

General Medical Council. (2017). Generic professional capabilities framework. *General Medical Council*. https://www.gmc-uk.org/-/media/documents/generic-professional-capabilities-framework--2109_pdf-70417127.pdf

Global e-Sustainability Initiative (GeSI). (2016). #SMARTer2030: ICT Solutions for 21st Century Challenges. *Global e-Sustainability Initiative*. https://gesi.org/research/smarter2030-ict-solutions-for-21st-century-challenges

*Gold, J., Thorpe, R., Woodall, J., & Sadler-Smith, E. (2007). Continuing professional development in the legal profession: A practice-based learning perspective. Management Learning, 38(2), 235–250. https://doi.org/10.1177/1350507607075777 *

*Goodrum, A. (2015). How to maneuver in the world of negative online reviews, the important ethical considerations for attorneys, and changes needed to protect the legal profession. *Information & Communications Technology Law*, *24*(2), 164–182. https://doi.org/10.1080/13600834.2015.1042568 *

*Graz, J.-C., & Hartmann, E. (2012). Transnational authority in the knowledge-based economy: Who sets the standards of ICT training and certification? *International Political Sociology*, *6*(3), 294–314. https://doi.org/10.1111/j.1749-5687.2012.00165.x *

Greenleaf, G. (2012). Global data privacy laws: 89 countries, and accelerating. *Privacy Laws & Business International Report*, (115), Special Supplement, February 2012. Queen Mary School of Law Legal Studies Research Paper No. 98/2012. https://www.researchgate.net/publication/228149428_Global_Data_Privacy_Laws_89_Countries_and_Accelerating

Greenwood, R., Suddaby, R., & Hinings, C. R. (2002). Theorising change: The role of professional associations in the transformation of institutionalised fields. *Academy of Management Journal, 45*(1), 58–80. https://doi.org/10.5465/3069285

*Gunther, S. V. (2014). The ethics of ethical regulation: Protecting the practitioner as well as the client. *Psychotherapy and Politics International, 12*(2), 111-128. https://doi.org/10.1002/ppi.1325 *

Hedges, L. V., & Olkin, I. (1985). *Statistical methods for meta-analysis*. Academic Press. https://doi.org/10.1016/c2009-0-03396-0

Hippocratic Oath. (2018). *Funk & Wagnalls New World Encyclopedia*, 1. https://www.newworldencyclopedia.org/entry/Encyclopedia

Information-Technology Promotion Agency (IPA). (2019). *Cybersecurity Workforce Development Initiative*. https://www.ipa.go.jp/en/it-talents/skill-standard/skill-framework-documents.html

International Engineering Alliance. (2014). *25 years of the Washington Accord: Celebrating international engineering education standards*. https://www.ieagreements.org/assets/Uploads/Documents/History/25YearsWashingtonAccord-A5booklet-FINAL.pdf

ISACA. (2020a). *Cyber insurance for a changing landscape*. ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/cyber-insurance-for-a-changing-landscape

ISACA. (2020b). *Leveraging cybersecurity to increase diversity, equity and inclusion*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/cybersecurity-workforce-diversity-including-cultures-personalities-and-neurodiversity

ISACA. (2021). *State of cybersecurity 2021, part 2: Threat landscape, security practices, and career impact*. ISACA. https://www.isaca.org/resources/infographics/state-of-cybersecurity-2021-part-2

ISC2. (2019). *Innovation through inclusion: The multicultural cybersecurity workforce*. ISC2. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/Innovation-Through-Inclusion-Report.pdf

ISC2. (2023). *2023 Cybersecurity Workforce Study*. https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study.pdf

ISC2. (2024). *Unified Body of Knowledge for the Cybersecurity Profession*. ISC². https://www.isc2.org/about/Unified-Body-of-Knowledge

Israel - National Cyber Security Framework. (2020). *Israel National Cyber Directorate*. https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

*Jankowski, J., Feldman, S. L., Morley, G., & Rose, S. L. (2020). Looking to other professions to advance the health care ethics consultant certification program. American Journal of Bioethics, 20(3), 21–24. https://doi.org/10.1080/15265161.2020.1714816 *

Janssens, C. (2013). *The principle of mutual recognition in EU law*. OUP Oxford. https://search.worldcat.org/title/The-principle-of-mutual-recognition-in-EU-law/oclc/863822814

Kim, J., & Park, C. (2020). Education, skill training, and lifelong learning in the era of technological revolution: a review. *Asian-Pacific Economic Literature*, *34*(2), 3–19. https://doi.org/10.2139/ssrn.3590922

*Knowles, W., Such, J., Gouglidis, A., Misra, G., & Rashid, A. (2017). All that glitters is not gold: On the effectiveness of cyber security qualifications. *Computer, 50*(12), 60-71. https://doi.org/10.1109/MC.2017.4451226 *

*Ko, C. (2009). Elevating IT's professional status. (cover story). *ComputerWorld Hong Kong*, *26*(9), 32–34. https://www.magzter.com/HK/Questex-Asia/Computerworld-Hong-Kong/Technology/ *

Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, W. (Eds.). (2020). The EU general data protection regulation (GDPR): A commentary. Oxford Academic. https://doi.org/10.1093/oso/9780198826491.001.0001

Light, R. J., & Pillemer, D. B. (1984). *Summing up: The science of reviewing research*. Harvard University Press. https://doi.org/10.3102/0013189x015008016

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allenby, B., & Klimek, M. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions, 33*(4), 471-476. https://doi.org/10.1007/s10669-013-9485-y

Loi, M., & Christen, M. (2019). Ethical frameworks for cybersecurity. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The ethics of cybersecurity* (pp. 47-68). Springer. https://doi.org/10.1007/978-3-030-29053-5_4

Manjikian, M. (2023). *Cybersecurity ethics: An introduction* (2nd ed.). Routledge. https://doi.org/10.4324/9781003248828

Moskowitz, D. (2022). *Fundamentals of adopting the NIST cybersecurity framework* (1st ed.). TSO. https://dokumen.pub/fundamentals-of-adopting-the-nist-cybersecurity-framework-9780117093706-011709370x.html

National Institute of Standards and Technology (NIST). (2020). *NICE cybersecurity workforce framework*. NIST Special Publication 800-181. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

National Research Council. (2013). *Professionalizing the nation's cybersecurity workforce? Criteria for decision-making*. The National Academies Press. https://doi.org/10.17226/18446

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework (NIST Special Publication 800-181). *National Institute of Standards and Technology.* https://doi.org/10.6028/NIST.SP.800-181

Nilsson, H. (2007). Professionalism, lecture 5: What is a profession? *University of Nottingham*. http://www.cs.nott.ac.uk/~nhn/G52GRP/LectureNotes/lecture05-4up.pdf

ÓhÉigeartaigh, S. S., Whittlestone, J., Liu, Y., Zeng, Y., & Liu, Z. (2020). Overcoming barriers to cross-cultural cooperation in AI ethics and governance. *Philosophy & Technology, 33*(4), 571-593. https://doi.org/10.1007/s13347-020-00402-x

*Ooi, K. B. (2006). A step towards the washington accord (1989)? International MultiConference of Engineers & Computer Scientists 2006, 630–635. https://www.researchgate.net/publication/220269917_A_step_towards_the_Washington_Accord_1989 *

Ozkaya, E. (2019). *Cybersecurity: The beginner's guide: A comprehensive guide to getting started in cybersecurity*. Packt Publishing. https://www.packtpub.com/en-us/product/cybersecurity-the-beginners-guide-9781789616194

Patil, A., & Codner, G. (2007). Accreditation of engineering education: Review, observations, and proposal for global accreditation. *European Journal of Engineering Education, 32*(6), 639–651. https://doi.org/10.1080/03043797.2007.11405001

*Passow, H. J., & Passow, C. H. (2017). What competencies should undergraduate engineering programs emphasize? A Systematic Review. Journal of Engineering Education, 106(3), 475–526. https://doi.org/10.1002/jee.20171 *

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy, 10*(3), 76–79. https://doi.org/10.1109/MSP.2012.84

Pearson, E. S. (n.d.). Book Reviews - "Student" A statistical biography of William Sealy Gosset. *Pearson, E.S.: Metrika. 40 1993*. https://eudml.org/doc/176454

Pfleeger, C. P., & Cunningham, R. K. (2019). *Security in computing (6th ed.)*. Pearson. https://www.pearson.com/en-us/subject-catalog/p/security-in-computing/P200000009559/9780137891214

Pfleeger, S. L., & Cunningham, R. K. (2010). Why measuring security is hard. *IEEE Security & Privacy, 8*(4), 46-54. https://doi.org/10.1109/msp.2010.60

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research, 20*(1), 121-139. https://doi.org/10.1287/isre.1080.0174

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the cyber security body of knowledge. *IEEE Security and Privacy*, *16*(3), 96-102. https://doi.org/10.1109/MSP.2018.2701150

*Reece, R. P., & Stahl, B. C. (2015). The professionalisation of information security: Perspectives of UK practitioners. *Computers & Security*, *48*, 182–195. https://doi.org/10.1016/j.cose.2014.10.007. *

Schein, E. H. (2017). *Organisational culture and leadership* (5th ed.). Wiley. https://www.wiley.com/en-nz/Organizational+Culture+and+Leadership%2C+5th+Edition-p-9781119212041

Schlag, P. V. (2004). Looking to the future: Standardized certifications. *Certification Magazine*, *6*(7), 20–23. https://www.certmag.com/

*Senior, C. (2009). Strategic professional development. *International Journal of Continuing Engineering Education and Life-Long Learning*, *3*(1/2). https://doi.org/10.1504/ijceell.1993.030272 *

Shoaib, S., Siddique, M., & Younis, S. (2024). Ethical dilemmas: A perspective from pakistani higher education institutions. *FWU Journal of Social Sciences*, *18*(3), 90–110. https://doi.org/10.51709/19951272/Fall2024/9

*Shukla, S. K., Kole, M., Upadhyay, A. K., Sinha, A., Sharma, P., Sarkar, M., Yadav, S. K., & Chourasia, S. R. (2024). Cybersecurity frameworks and models: Review of the existing global best practices. Productivity, 65(1), 29–42. https://doi-org.edgewood.idm.oclc.org/10.32381/PROD.2024.65.01.4 *

SkillsFuture Singapore. (2019). *Skills framework for infocomm technology – cybersecurity*. https://www.skillsfuture.gov.sg/skills-framework/ict

Spinner, J. (2010). Speaking of certification. *Consulting Specifying Engineer*. https://www.csemag.com/articles/speaking-of-certification/

SRA Solicitors Regulation Authority. (2018a). *SRA Standards and Regulations, Principles*. https://www.sra.org.uk/solicitors/standards-regulations/principles/

SRA Solicitors Regulation Authority. (2018b). *SRA Good Standing and Certifications, Certificates*. https://www.sra.org.uk/goodstanding

Steven, K., Howden, S., Mires, G., Rowe, I., Lafferty, N., Arnold, A., & Strath, A. (2017). Toward interprofessional learning and education: Mapping common outcomes for prequalifying healthcare professional programs in the United Kingdom. *Medical Teacher*, *39*(7), 720–744. https://doi.org/10.1080/0142159X.2017.1309372

Sweeney, P., & McFarlin, D. (2014). *International management: Strategic opportunities and cultural challenges* (5th ed.). Routledge. https://doi.org/10.4324/9780203406496

Taddeo, M. (2017). Data philanthropy and the design of the ethics of AI. *Philosophy & Technology, 30*(1), 111-116. https://doi.org/10.1098/rsta.2016.0113

Taherdoost, H. (2024). Towards an innovative model for cybersecurity awareness training. *Information (2078-2489)*, *15*(9), 512. https://doi.org/10.3390/info15090512

Tretko V, Vashkurak Y, Gorbenko A. (2020). Professional certification and advanced training of cybersecurity professionals in the UK. *Comparative Professional Pedagogy*. 2020;10(4):38-46. doi:10.3189/2308-4081/2020-10(4)-5

Tseng, P. T., Chen, Y. W., Chung, W., Tu, K. Y., Wang, H. Y., Wu, C. K., & Lin, P. Y. (2016). Significant effect of valproate augmentation therapy in patients with schizophrenia: A meta-analysis study. *Medicine*, *95*(4), e2475. https://doi.org/10.1097/MD.0000000000002475

*Udeh, I. E. (2016). The gap between perceived value of information technology certification and the persistence applied to achieve such certification. *International Journal of Business Research & Information Technology (IJBRIT)*, *3*(1), 1–17. https://www.iabpad.com/the-gap-between-perceived-value-of-information-technolgy-certification-and-the-persistence-applied-to-achieve-such-certification/ *

UK Cyber Security Council. (2021). *Cybersecurity career pathways framework*. https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/

Umbrello, S. (2017). Designing in ethics. *Prometheus, 35*(2), 160-161. https://doi.org/10.1080/08109028.2018.1486470

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Washington Accord. (2021). *Graduate Attributes & Professional Competences.* International Engineering Alliance. http://www.ieagreements.org/

Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security (6th ed.)*. Cengage Learning. https://www.researchgate.net/publication/200446660_Principles_of_Information_Security

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. N*ational Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-50

Woods, D. D., & Hollnagel, E. (2017). *Resilience engineering: Concepts and precepts*. CRC Press. https://doi.org/10.1201/9781315605685

World Economic Forum. (2020). *Why cybersecurity needs a more diverse and inclusive workforce*. World Economic Forum. https://www.weforum.org/stories/2021/10/why-cybersecurity-needs-a-more-diverse-and-inclusive-workforce/

Bibliography

American Psychological Association. (2020). *Publication manual of the American Psychological Association* (7th ed.). https://doi.org/10.1037/0000165-000

Barber, B. (1963). *The logic and limits of trust*. Rutgers University Press. DOI: https://doi.org/10.2307/1961263

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs, 92*(1), 43-62. https://doi.org/10.1111/1468-2346.12504

Carr-Saunders, A. M., & Wilson, P. A. (1933). *The professions*. Oxford University Press. https://doi.org/10.2307/2224787

Chen, T., & Zhang, X. (2020). The professionalisation of cybersecurity: Establishing certification standards and ethical guidelines. *Journal of Cybersecurity Education*, *6*(2), 145-160. https://doi.org/10.1093/cybsec/qbaa024

Christou, G. (2016). The EU's approach to cyber security. *Journal of Information Warfare, 15*(2), 81-96. https://www.semanticscholar.org/paper/The-EU's-Approach-to-Cybersecurity-Christou/4f1ed6b053c7c8d0a882277515b2ce393a7a19fe

CONNECTING ASIA TV. (2021, July 22). *Basics of meta-analysis* [Video]. YouTube. https://www.youtube.com/watch?v=dssBmD9jp6c

Creese, S., Dutton, W. H., Esteve-González, P., & Shillair, R. (2021). Cybersecurity capacity-building: cross-national benefits and international divides. *Journal of Cyber Policy*, *6*(2), 214–235. https://doi.org/10.1080/23738871.2021.1979617

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations. *International Studies Review, 8*(3), 543-547. https://doi.org/10.1177/0192512106064462

Field, Andy P., and Raphael Gillett. 2010. “How to Do a Meta-Analysis.” *British Journal of Mathematical & Statistical Psychology* 63 (3): 665–94. https://doi.org/10.1348/000711010X502733.

Goode, W. J. (1960). Encroachment, charlatanism, and the emerging profession: Psychology, sociology, and medicine. *American Sociological Review*, *25*(6), 902-914. https://doi.org/10.2307/2089984

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC), 5*(4), 438-457. https://doi.org/10.1145/581271.581274

Hedges, L. V. (1981). Distribution theory for Glass’s estimator of effect size and related estimators. *Journal of Educational Statistics, 6*(2), 107–128. https://doi.org/10.2307/1164588

Hoyle, E. (2001). Teaching: Prestige, status and esteem. *Educational Management & Administration*, *29*(2), 139–152. https://doi.org/10.1177/0263211X010292004

Johnson, T. J. (1972). *Professions and power*. Macmillan. https://api.pageplace.de/preview/DT0400.9781315471365_A27016659/preview-9781315471365_A27016659.pdf

Krause, E. A. (1996). *Death of the guilds: Professions, states, and the advance of capitalism, 1930 to the present*. Yale University Press. https://doi.org/10.1056/nejm199708213370821

LajeunesseLab. (2021, March 2). *Tutorial on how to do a meta-analysis in Excel | Spreadsheet Synthesis* [Video]. YouTube. https://www.youtube.com/watch?v=i66Lf2a_Pa8

Lauder, L., & Neary, S. (2020). The Role and Relevance of Theory in Careers Professionalisation and Practice. *British Journal of Guidance & Counselling*, *48*(4), 477–488. https://doi.org/10.1080/03069885.2020.1750560

Matysiak, A., & Vignoli, D. (2008). Fertility and women's employment: A meta-analysis. *European Journal of Population, 24*(4), 363–384. https://doi.org/10.1007/s10680-007-9146-2

McMillan, J. H., & Schumacher, S. (2010). *Research in education: Evidence-based inquiry* (7th ed.). Pearson. https://eric.ed.gov/?id=ED577250

stikpet. (2022, July 25). *Excel - Hedges g (one-sample)* [Video]. YouTube. https://www.youtube.com/watch?v=7QPTBuCn1wg

Stine, K., Quinn, S., Witte, G., & Gardner, R. (2020). Integrating cybersecurity and enterprise risk management (ERM). *NIST Interagency/Internal Report (NISTIR)*. National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.8286

Susskind, R., & Susskind, D. (2015). *The future of the professions: How technology will transform the work of human experts*. Oxford University. https://doi.org/10.7146/tfa.v20i3.110817

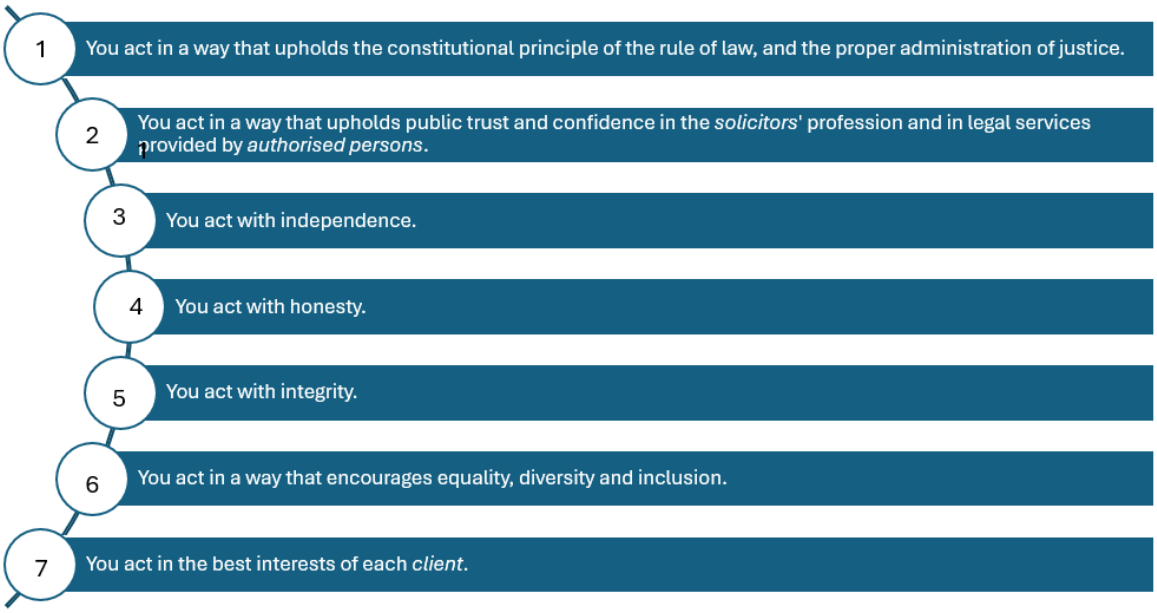
Appendix A

Washington Accord – Graduate Attributes

Note: Based on International Engineering Alliance. (2014), pp 14-15.

Appendix B

Solicitors Regulation Authority, U.K. - The Seven Principles



Note: Based on SRA Solicitors Regulation Authority. (2018a).

Appendix C

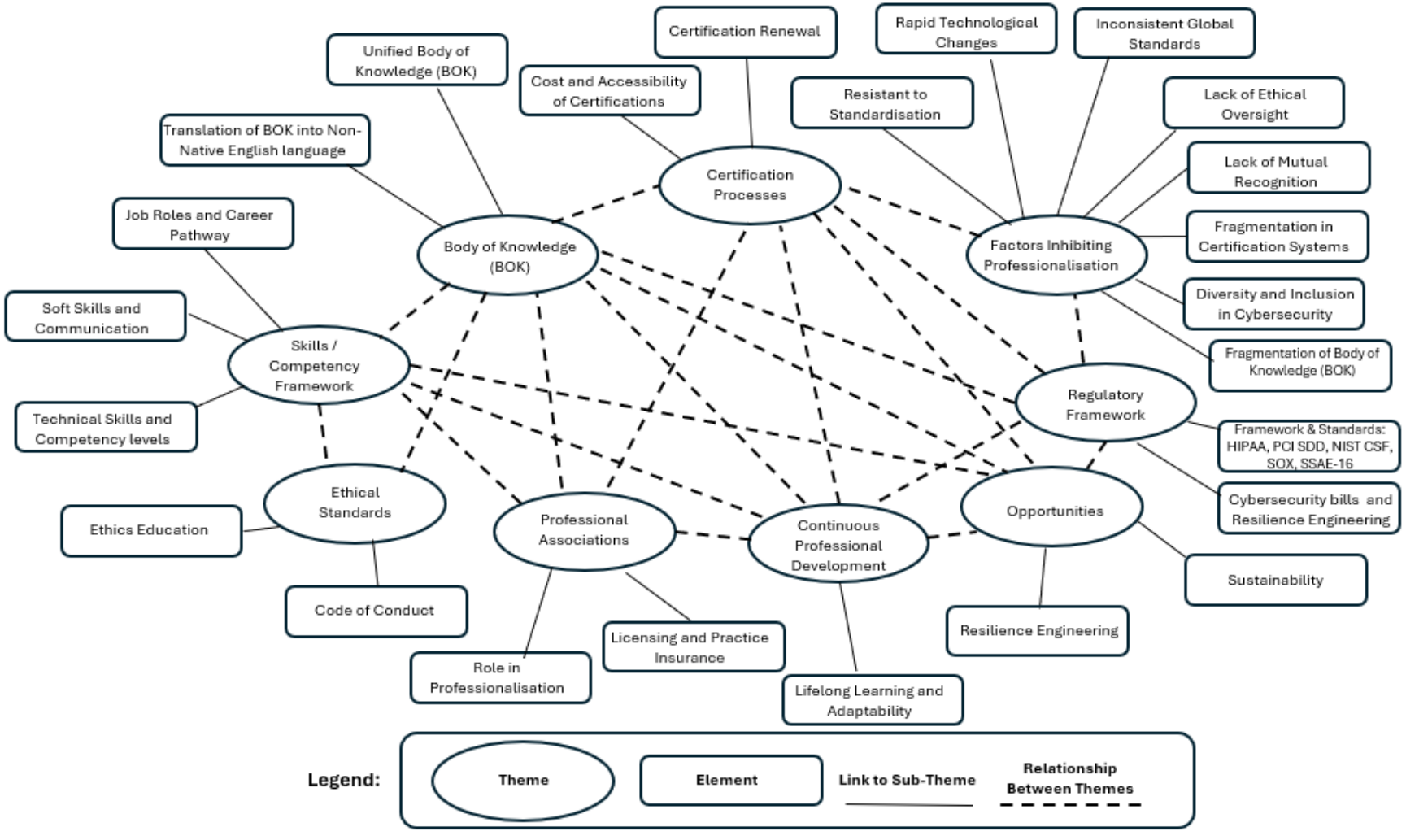
General Medical Council, U.K. – Professional Values and Behaviours

Note: Adapted from General Medical Council (2017), p5. In the public domain.

The Generic professional capabilities framework has three fundamental domains: (1) professional values and behaviours; (2) professional skills; and (3) professional knowledge.

Appendix D

Thematic Analysis of Professionalisation Framework



Appendix E

IRB Approvals and Consent Form

Consent Form

Since this study did not use human participants, no consent forms were needed.

Statement of Consent

No statements of consent were required for this study.

Participant Bill of Rights

No participants were used in this study.