Towards the Integration of Cyber Security and Enterprise Architecture to Improve Cyber Risk Management

Thesis · January 2025

DOI: 10.5281/zenodo.14639415

1 author:

Nick Nieuwenhuis
University of Applied Sciences Utrecht
1 PUBLICATION **0** CITATIONS

SEE PROFILE

HU University of Applied Sciences

Master of Informatics

Towards the Integration of Cyber Security and Enterprise Architecture to Improve Cyber Risk Management

Master's Thesis

Author: Nick Nieuwenhuis

Lecturer: Prof. dr. ir. Johan Versendaal
Supervisor: Dr. Ir. Raymond Slot MBA
Co-Supervisor: Edzo Botjes, MSc

Date: 9 January 2025
DOI: https://doi.org/10.5281/zenodo.14639415

HU University of Applied Sciences
P.O. box 182
3500 AD UTRECHT
The Netherlands

Towards the Integration of Cyber Security and Enterprise Architecture to Improve Cyber Risk Management

Nick Nieuwenhuis

2025

Acknowledgements

The past two years have been filled with remarkable experiences, culminating in the completion of this thesis as part of the Master of Informatics (MOI) program. I feel incredibly fortunate to have been surrounded by supportive individuals, without whom this journey would not have been possible. I would like to take this opportunity to express my gratitude to those who provided invaluable guidance and encouragement along the way.

First, I extend my deepest gratitude to my girlfriend, Cécile, for her unwavering support. From initially encouraging me to pursue a master's degree alongside my professional and personal commitments, to keeping me motivated and inspired throughout the research process, your belief in me has been a constant source of strength. A special shout-out for your critical view on inconsistencies in this thesis. Thank you for your patience and understanding, especially when I needed to dedicate late nights and weekends to this thesis, often at the expense of our time together.

I would also like to thank Raymond Slot, Lecturer of the Cyber Security Lectorate at HU University of Applied Sciences, for his insightful supervision and ongoing feedback. Your expertise and support have been invaluable in shaping this research, ensuring both academic rigor and practical relevance.

A special note of gratitude goes to Edzo Botjes. Your introduction to Enterprise Architecture and Complexity Sciences sparked my interest in exploring the intersection of Enterprise Architecture and Cyber Security, which formed the foundation of this research. I deeply appreciate your continuous guidance and constructive feedback, which contributed to the quality of this thesis. Working with you has been an enlightening experience, and I have gained significant knowledge in both the academic and practical aspects of EA and Security.

I would also like to extend my thanks to HU University of Applied Sciences for the opportunity to conduct this research, and to Marlies van Steenbergen and Jeroen van Grondelle for their critical feedback during the thesis proposal phase. Additionally, I am grateful to my employers, HSO and Nedscaper, for their support in allowing me to pursue this degree alongside my professional responsibilities.

A special thanks is due to Rick Tijsterman for his assistance with the Meetingwizard application. Your guidance in navigating its features was instrumental in the successful preparation and execution of the Focus Group.

Finally, I would like to express my appreciation to all the participants in this research. I am sincerely grateful to those who took time out of their busy schedules to contribute their insights. Your input was invaluable, and I hope the findings of this research resonate with you.

Abstract

Enterprises are facing increasingly complex cyber risks that form a threat to business continuity. Prior research suggests that integrating Cyber Security and Enterprise Architecture can improve Risk Management but provides limited guidance on *how* Cyber Security and Enterprise Architecture should be integrated.

This research explores the integration of Cyber Security and Enterprise Architecture and examines its impact on Cyber Risk Management. A qualitative research approach was chosen, with data collected through a Focus Group and four Interviews with experts in the field. Thematic analysis was used to identify key strategies that enterprises employ to facilitate the integration and improve Cyber Risk Management.

The findings reveal that Cyber Security and Enterprise Architecture are currently 'somewhat integrated'. Blockers to this integration include different mindsets and focuses, organizational misalignment, and skills and knowledge gaps. Conversely, embedding security into Enterprise Architecture frameworks, aligning organizational structures, and adopting secure development practices were identified as critical to improving the integration. Four key strategies were derived from the data that contribute to this integration:

1. **Embedding Cyber Security into Enterprise Architecture Frameworks:** Integrating security considerations, such as principles, viewpoints, and requirements, as a fundamental part of EA frameworks ensures security is a primary concern in the architectural development process and not an afterthought.
2. **Leveraging agile and secure development methodologies:** Agile and secure development methodologies such as Security by Design and DevSecOps ensure enterprises can implement Cyber Security measures proactively.
3. **Improving in-depth knowledge in Cyber Security and Enterprise Architecture teams**: Improving architectural knowledge on the Cyber Security level and improving in-depth Cyber Security knowledge at the Enterprise Architecture level is crucial for shared understanding, awareness, and knowledge exchange.
4. **Aligning Cyber Security and Enterprise Architecture functions in the Organizational Structure**: Creating a shared vision, strategy, mindset, and focus between the Cyber Security and Enterprise Architecture functions can enhance collaboration and joint decision making.

Furthermore, this study found that the effective integration of Cyber Security and Enterprise Architecture leads to improved Cyber Risk Management by enabling enterprises to more efficiently identify, assess, and address cyber risks at every stage of the Cyber Risk Management process. This research contributes to the field by providing practical insights and a list of strategies for overcoming integration challenges, supporting enterprises in improving their Cyber Risk Management capabilities.

Table of contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Definition
ADM	Architecture Development Method
CISO	Chief Information Security Officer
CRA	Cyber Resilience Act
CRM	Cyber Risk Management
CS	Cyber Security
CSF	Cyber Security Framework
EA	Enterprise Architecture
EAD	Enterprise Architecture Description
EAF	Enterprise Architecture Framework
EE	Enterprise Engineering
EEA	Enterprise Ecological Adaptation
EI	Enterprise Integrating
EISA	Enterprise Information Security Architecture
EITA	Enterprise IT Architecting
ERM	Enterprise Risk Management
GSS	Group Support System
ISO	International Standardization Organization
ISM	Information Security Management
IT	Information Technology
LR	Literature Review
NIS2	Network and Information Systems 2
NIST	National Institute of Standards and Technology
O-AA	Open Agile Architecture
RM	Risk Management
RQ	Research Question
SABSA	Sherwood Applied Business Security Architecture
TOGAF	The Open Group Architecture Framework

Glossary of Terms

Term	Definition
Computer Security	The protection of system data and resources from accidental and deliberate threats to confidentiality, integrity, and availability.
Cyber Security	Securing information and noninformation assets that are within cyberspace or could be affected via cyberspace.
Cyberspace	The collection of all networked or interconnected information systems.
Cyber Risk	An operational risk associated with the performance of activities in cyberspace, threatening information assets, ICT resources and technological assets, which may cause material damage to tangible and intangible assets of an organization.
Cyber Risk Management	Coordinated activities to direct and control an organization with regards to cyber risk.
Enterprise	An intentionally created entity of human endeavor with a certain purpose.
Enterprise Architecture	Fundamental concepts or properties [of an enterprise] in its environment and governing principles for the realization and evolution [of this enterprise] and its related life cycle processes.
Risk Management	Coordinated activities to direct and control an organization with regards to risk.
Information Security	The protection of information from possible harm resulting from various threats and vulnerabilities.
Operational Risk	The risk of loss resulting from inadequate or failed processes, people, and systems or from external events.

1 Introduction and Background

Over the past 25 years, cyber risks have evolved from mere annoyances to catastrophic events, posing challenges for enterprises worldwide (Dupont et al., 2023; Sun et al., 2023). Enterprises are increasingly reliant on information technology (IT) assets to deliver value to their customers (Cebula et al., 2010; Steenbergen, 2023). Failure of these assets can impact the objectives of an enterprise and threaten business continuity (Giuca et al., 2021; Soomro et al., 2016). A clear example of this is the CrowdStrike outage in 2024, which brought enterprise worldwide to a standstill (George, 2024). This is further highlighted by the World Economic Forum's 2024 Global Risks Report, which ranks '*cybercrime and cyber insecurity*' as the fourth most severe global risk (World Economic Forum, 2024). Common cyber risks targeting enterprises are ransomware, phishing, insider threats and espionage (Dupont et al., 2023; Eling et al., 2023).

Research by the IBM Ponemon Institute reports that the global average cost of a data breach reached an all-time high of $4.88 million in 2024, including direct costs, such as system downtime and lost business, and indirect costs, like legal fees and recovery expenses (IBM, 2024). This marks a significant increase of more than 26% compared to 2020, when the average cost of a data breach was $3.86 million, see Figure 1.

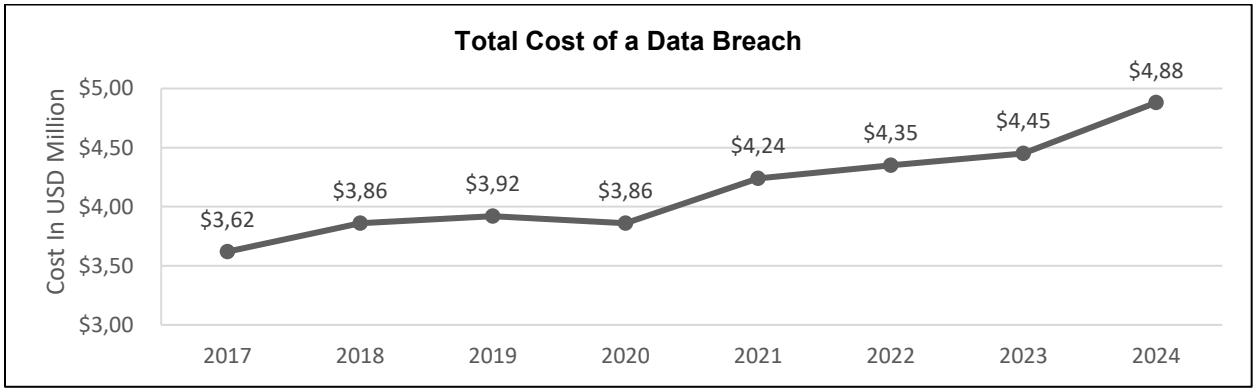

Figure 1. Total Average Cost of a Data Breach in USD Million (IBM, 2024)

Cyber risks continue to evolve, introducing new challenges related to emerging technologies such as Quantum Computing and Post-Quantum Cryptography (PQC), as well as Artificial Intelligence (AI) and Machine Learning (Admass et al., 2024). To add to the complexity, enterprises must be compliant with an increasing number of Cyber Security (CS) law and regulations, such as the *Network and Information Systems 2* (NIS2) directive (European Parliament, 2022) and the *Cyber Resilience Act* (CRA) (Boeken, 2024; European Commission, 2022). These evolving risks and regulatory requirements underscore the need for a holistic approach to manage cyber risks (Eling et al., 2021; Mayer et al., 2015; Ruan, 2019).

Enterprise Architecture (EA) is a promising vehicle to manage cyber risks holistically because EA is often seen as a comprehensive blueprint of the enterprise that encompasses the Business, Data, Application, and Technology domains (Kotusev et al., 2022; Kurnia et al., 2020). Adopting an EA framework, such as The Open Group Architecture Framework (TOGAF), can aid in this challenge; however, the practical value of these frameworks remains insufficiently understood (Kotusev, 2018). CS is often considered a cross-cutting concern within EA, overarching the Business, Data, Application, and Technology domains (Kotusev et al., 2024; The Open Group, 2022c). Therefore, incorporating CS into EA can benefit enterprises by ensuring that security is embedded into all aspects of information system design (Loft et al., 2022).

Despite these benefits, integrating CS and EA is a challenge for enterprises, as CS often dwells in functional silos (Falco et al., 2019; Stine et al., 2020). Such siloed implementations result in ineffective Cyber Risk Management (CRM), leaving enterprises vulnerable (Althonayan & Andronache, 2018; Graham et al., 2021; McClintock et al., 2020). To continuously deliver value to stakeholders, enterprises must effectively manage cyber risks (Lee, 2021; Ruan, 2019).

1.1 Problem Statement

To guide this research, I have developed the following problem statement:

The lack of integration between Cyber Security and Enterprise Architecture negatively impacts Cyber Risk Management, leaving enterprises at risk.

Prior research on integrating CS and EA focused mostly on '*why'* this integration should happen, but '*how'* this integration should look like, remains inadequately understood (Diefenbach et al., 2019; Loft et al., 2021). The aim of this research is to identify strategies that enterprises can use to integrate CS and EA, and to evaluate how this integration impacts CRM. Documenting these strategies can help enterprises improve this integration, ultimately leading to more secure enterprises (Diefenbach et al., 2019; Giuca et al., 2021; Loft et al., 2021; Soomro et al., 2016).

1.2 Research Questions

To frame this research, I have developed the following main Research Question:

How can Cyber Security and Enterprise Architecture be integrated in relation to Cyber Risk Management within enterprises?

To address this question, four sub-questions (SQs) are formulated, as shown in Table 1. SQ1 investigates how Cyber Security and Enterprise Architecture are currently integrated within organizations. SQ2 and SQ3 explore the common blockers and enablers of this integration. SQ4 examines how this integration may influence Cyber Risk Management. Collectively, answering these sub-questions will provide insights into the main research question. The research methodology and methods for answering these questions are detailed in Chapter 3.

Table 1. *Overview of Sub-questions*

Nr.	Sub-question
SQ1	How are Cyber Security and Enterprise Architecture currently integrated within enterprises?
SQ2	What are blockers for the integration of Cyber Security and Enterprise Architecture?
SQ3	What are enablers for the integration of Cyber Security and Enterprise Architecture?
SQ4	What is the impact of the integration of Cyber Security and Enterprise Architecture on Cyber Risk Management?

1.3 Reading Guide

This thesis is structured as follows:

- Chapter 2 provides the theoretical background on the core concepts of Cyber Security, Enterprise Architecture, and Cyber Risk Management;
- Chapter 3 outlines the research methodology and methods employed in this study;
- Chapter 4 presents the empirical findings, summarizing the outcomes of the Focus Group and expert interviews;
- Chapter 5 discusses the key findings, comparing them to existing literature and addressing their scientific implications;
- Chapter 6 concludes the thesis by synthesizing the key outcomes, answering the main research question, and documenting practical implications, limitations, and directions for future research.

The appendices contain additional details relevant to this research, as referenced throughout the text.

2 Theoretical Background

This section describes the conceptual model and research proposition that was developed to guide this research, as well as the Literature Review on the current body of knowledge of Cyber Security (CS), Enterprise Architecture (EA) and Cyber Risk Management (CRM).

2.1 Conceptual Model and Theoretical Lens

Before I delve into the Theoretical Background of my research, I want to introduce the conceptual model because this model visualizes the theoretical lens through which I will be examining my research problem, see Figure 2.

Figure 2. Conceptual Model

The conceptual model shows that 'Integrated Cyber Security (CS) and Enterprise Architecture (EA)' impacts 'Cyber Risk Management (CRM)'. The aim of this study is to find ways, or strategies, that can facilitate this integration by removing blockers and stimulating enablers, ultimately enhancing the integration of CS and EA and therefore CRM too.

2.2 Research Proposition

While evidence on how integrated CS and EA impacts CRM is limited, this research suggests that integrating CS and EA can positively impact CRM, so that enterprises are better equipped to address cyber risks holistically rather than in isolation. In contrast, if CS and EA are not integrated, this will negatively impact CRM and therefore exposing enterprises to cyber risks. This research proposition will be explored through a comprehensive Literature Review, supported by empirical evidence from experts and practitioners. A reflection on this proposition can be found in Chapter 5: Discussion.

2.3 Cyber Security

This section provides an overview of the history of Cyber Security (CS), encompassing various definitions, its relationship with information security, and key concepts and frameworks that are important to this research.

2.3.1 History of Cyber Security

CS research started in the late 1960s, when the first version of the internet – the ARPANET - was launched (Eling et al., 2021; Roberts, 1986). In 1970, the first report on Computer Security was published by the American Department of Defense. This report concluded that comprehensive security of computers requires a combination of hardware, software, physical, communication, personnel, and administrative controls (Ware, 1970). The protection of information within the ARPANET was mainly achieved through the control of physical access to computers, accompanied with technical measures such as encryption (Samonas & Coss, 2014; Shankar, 1977). Ruthberg and McKenzie (1977, p. 11-4) defined Computer Security as "*The protection of system data and resources from accidental and deliberate threats to confidentiality, integrity, and availability*". There was a shift in the focus from the protection of computers to the protection of information, as the cost of computer technology decreased, and the use of computers increased (Samonas & Coss, 2014, p. 23). The term Computer Security eventually evolved into many different terms and became 'Information Security' in 2001 (Blakley et al., 2001) and 'Cyber Security' In 2013 (Von Solms & Van Niekerk, 2013).

2.3.2 Defining Cyber Security

Von Solms and van Niekerk (2013, p. 97) argue that "*although Information Security and Cyber Security are used interchangeably, a nuanced difference exists between the two concepts.*" Information Security can be defined as: "*The protection of information from possible harm resulting from various threats and vulnerabilities*" (von Solms & van Niekerk, 2013, p. 101).

The scope of CS goes beyond Information Security by also protecting non-information assets that are vulnerable to threats via Information and Communication Technology (ICT) (Von Solms & Van Niekerk, 2013). To give an example, the protection of paper documents is part of Information Security and not part of CS, unless these papers are also digitally stored (von Solms & von Solms, 2018). The International Organization for Standardization (ISO, 2023, p. 2) defines Cyber Security as "*the preservation of the confidentiality, integrity, and availability of information in cyberspace.*" As von Solms and von Solms (2018, p. 4) state: "*The difference between Cyber Security and Information Security is that Cyber Security is restricted to the information in cyberspace; whereas Information Security is the protection of information 'everywhere',*" see Figure 3.

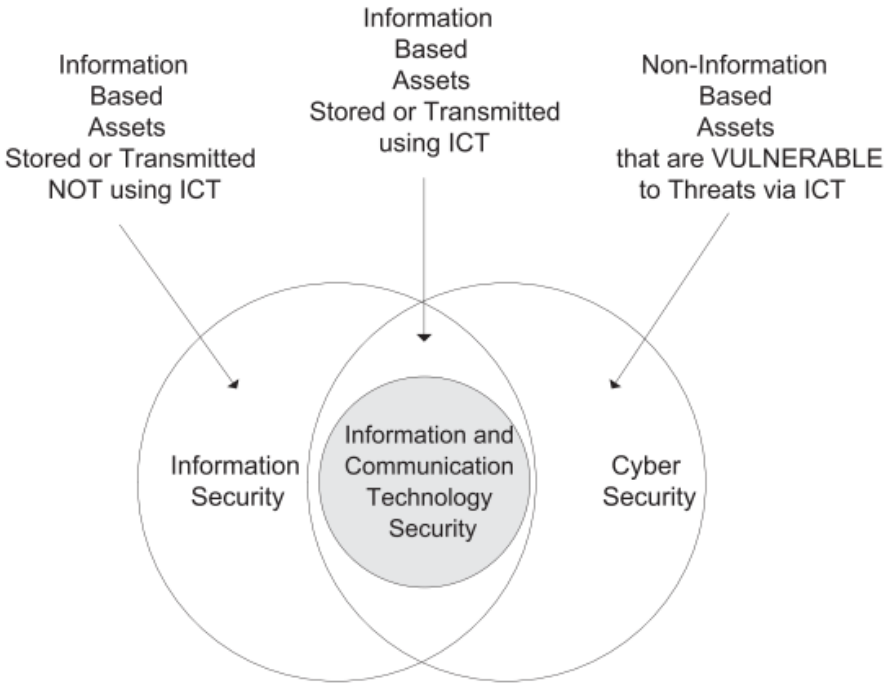

Figure 3. The Difference between Information Security and Cyber Security (von Solms & van Niekerk, 2013)

Eling et al. (2021, p. 95) have adopted this difference and define Cyber Security as: *"Securing information and noninformation assets that are within cyberspace or could be affected via cyberspace".* Examples of noninformation assets are humans who can be compromised (e.g., through social engineering) and physical assets that can be damaged using cyberspace, for example through Ransomware attacks (Eling et al., 2021). Cyberspace can be defined as the collection of all networked or interconnected information systems (Eling et al., 2021; Giuca et al., 2021; Zhang et al., 2015). Since this research focuses on CS, the definition provided by Eling et al. (2021), which is based on the definition of von Solms and van Niekerk (2013), will be used going forward.

2.3.3 Cyber Security Concepts

Given the strong interconnection between CS and Risk Management, understanding the fundamental concepts underlying both fields is essential (Diefenbach et al., 2019; Loft et al., 2022; Refsdal et al., 2015). The following list describes the core CS concepts of asset, threat, control, and vulnerability in more detail.

1) **Asset:** An asset is something of value to an organization. This can be anything, ranging from hardware (e.g., devices, servers), software (e.g., applications), information and data (e.g., intellectual property), infrastructure, and people (ISO, 2022b). In other words, assets are the objects that need protection because they contribute to the organization's mission and objectives (Refsdal et al., 2015).

2) **Threat:** A threat is a potential event that can harm or reduce the value of an asset or the organization altogether (ISO, 2022b; Refsdal et al., 2015). A threat is characterized by specific parameters such as a source of threat, actor, motives of the actor and the location (Strupczewski, 2021). Examples of cyber threats are ransomware, malware, and data breaches (Cremer et al., 2022; Dupont et al., 2023). When a threat is realized and has an impact on an asset, it becomes an incident (ISO, 2022b).

3) **Control:** A control is a measure that maintains and/or modifies cyber risk (ISO, 2022b; Refsdal et al., 2015). Modification of a cyber risk can happen by eliminating the risk altogether, or by reducing the probability and/or impact (ISO, 2022b). Examples of controls are security policies, processes, and technological measures, such as access control, encryption, and firewalls (Alcántara & Melgar, 2016).

4) **Vulnerability:** A vulnerability is a weakness in an asset or control that can be exploited or misused (ISO, 2022b; Refsdal et al., 2015). Examples of vulnerabilities include programming mistakes, software misconfiguration, social engineering, and weak passwords (Böhme et al., 2019).

Refsdal et al. (2015) combine these CS concepts with the basic Risk concepts of ***probability*** (the chance of a risk to occur) and ***impact*** (the consequence of an incident on an asset in terms of harm or reduced asset value), as can be seen in Figure 4. Refsdal et al. (2015, p. 11) explain that "*the relation represented by a line with a black diamond connecting **risk** and **impact** captures that **impact** is an ingredient that belongs to **risk**. An **incident** may give rise to several **risks**. **Risk** is therefore connected to **incident** with a white diamond to express that although incident is an ingredient of **risk**, it does not necessarily belong uniquely to one **risk.***"

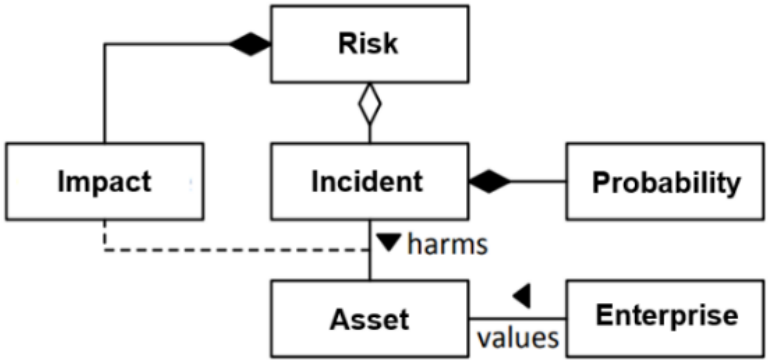

Figure 4. General Risk Concepts (Refsdal et al., 2015)

In this research, I intentionally only look at the downside of risk. While Refsdal et. al (2015) and the International Organization for Standardization (ISO, 2022) note that risks can have upsides, such as when balancing risk and opportunity for potential gain, Eling et al. (2021) argue that more research is needed to determine whether this applies to cyber risk too.

2.3.4 Cyber Security Frameworks

International organizations, academic institutions, and countries have been actively working to develop Cyber Security Frameworks (CSFs) (Azmi et al., 2018; Jarjoui & Murimi, 2021). CSFs offer guidance by giving examples of security policies, controls, and processes that enterprises can use to improve their CS capabilities (Giuca et al., 2021; ISO, 2022b). Common CSFs used in practice are the National Institute of Standards and Technology (NIST) CSF and the International Organization for Standardization (ISO) 27001 series on Information Security management (Giuca et al., 2021).

The NIST CSF has been recently updated to include the 'Govern' function, which is the function "*that addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy,"* see Figure 5 (NIST, 2024). The 'Govern' function highlights the importance of CS governance and Risk Management, making it a relevant function for EA, as will be explained in section 2.6.

Figure 5. NIST Cyber Security Framework (NIST, 2024)

Limitations of Cyber Security Frameworks

The literature identifies several limitations regarding CSFs including: 1) the lack of coherent taxonomy between frameworks (Loft et al., 2022), 2) siloed implementations of cybersecurity efforts (Althonayan & Andronache, 2019), and 3) lack of quantitative Cyber Risk Management (CRM) that justifies CS investments (Lee, 2021). Furthermore, most CSFs do not explicitly address the CS ecosystem, such as customers, supply chain partners, regulatory agencies, and its impact on CRM (Lee, 2021). Jarjoui and Murimi (2021) highlight a gap between theoretical frameworks and their practical application, suggesting that while CSFs provide valuable high-level guidance for implementation, they should be approached with caution.

2.4 Enterprise Architecture

Despite growing interest in Enterprise Architecture (EA), a lack of common understanding is frequently described by EA researchers and practitioners (Saint-Louis et al., 2019). In this section, I give a brief history of EA, different definitions, schools of thought, EA concepts, and EA frameworks relevant to this research.

2.4.1 History of Enterprise Architecture

When researching EA many publications mention John Zachman's '*A Framework for Information Systems Architecture*' (Zachman, 1987) as the first EA framework (Kotusev, 2016b). However, according to Kotusev (2016b, p. 29), "*the earliest origins of the modern concept of EA can be traced back to the Business Systems Planning (BSP) methodology initiated by IBM in the 1960s*." One of the most important resemblances is that BSP describes the relationship between organization, business processes, data, and information systems (Kotusev, 2016b). These four domains where later used in the PRISM EA framework (PRISM, 1986). After PRISM, many EA frameworks emerged, including the Zachman Framework, the NIST EA Framework and The Open Group Architectural Framework (TOGAF) (Kotusev, 2016b; Proper & Lankhorst, 2014). TOGAF has gained prominence as the most well-known framework for EA (Kotusev, 2016a).

2.4.2 Defining Enterprise Architecture

Although the word 'Enterprise' has been mentioned a few times already in this thesis, I have not defined what an 'Enterprise' is. Hoogervorst (2009, p. 4) defines an enterprise as: *"An intentionally created entity of human endeavor with a certain purpose."* Examples of enterprises are organizations, companies, businesses, and institutions (Hoogervorst, 2009, p. 4).

To get a grip on the complexity of any enterprise or system, an architecture is needed (Jonkers et al., 2006). EA can be used to bridge the technical and business-oriented views on CS (Innerhofer-Oberperfler & Breu, 2006), as well as manage complexity and drive digital transformation (Plessius et al., 2018). The term 'architect' is most known in the context of building architecture, where "*the architect specifies the spatial structure, dimensions, functions, materials, colors, and construction of a building, based on the requirements of its future owners and users, and in accordance with applicable regulations*" (Jonkers et al., 2006, p. 63). EA "*provides normative guidance for enterprise design, in order for the enterprise to operate as a unified and integrated whole, whereby various enterprise objectives must be satisfied"* (Hoogervorst, 2009, p. 8). EA is claimed to provide a vehicle for aligning and integrating strategy, people, business, and technology, and enabling an agile enterprise that is continually evolving within the ever-changing environment (Proper & Lankhorst, 2014). In the literature, many different definitions of EA exist, but most definitions lack uniformity, scope, and purpose (Saint-Louis et al., 2019). A summary of EA definitions can be found in Table 2.

Table 2. *Definitions of EA in Literature*

Source	Definition
Ross et al. (2006, p.9)	"The organizing logic for business processes and IT infrastructure, reflecting the integration and standardization requirements of the company's operating model."
Kotusev (2019, p. 1)	"EA is intended to bridge the gap between business and IT stakeholders and improve Business and IT alignment."
Niemi (2006, p. 1)	"EA includes all the models needed in managing and developing an organization, and takes a holistic view of its business processes, information systems and technological infrastructure."
Hoogervorst (2009, p. 297)	"A coherent and consistent set of principles and standards that guide enterprise design."
ISO 42010 (2022c, p. 2)	"Fundamental concepts or properties [of an enterprise] in its environment and governing principles for the realization and evolution [of this enterprise] and its related life cycle processes."

Lapalme (2012) recognizes the different definitions of EA and has developed three schools of thought, see Table 3. These schools of thought are non-exhaustive, but each school of thought has its own belief system, including definitions, concerns, assumptions, and limitations (Lapalme, 2012). Understanding and acknowledging these different schools of thought is important, because of the meaning EA will have on the construction and conceptualization of EA maturity within organizations (Vallerand et al., 2017).

Table 3. *EA Schools of Thought (Lapalme, 2012)*

School of Thought	Description
Enterprise IT Architecting (EITA)	EA is the glue between business and IT and an enabler for executing business strategy. This school of thought is about business and IT alignment, operational efficiency, and cost reduction. (Korhonen et al., 2016; Lapalme, 2012)
Enterprise Integrating (EI)	EA links strategy with execution and is used to not only enable enterprise strategy, but to implement it. Systems thinking is embedded within this school of thought. The organizational environment is considered, and Enterprise Integrating tries to manage that environment. (Korhonen et al., 2016; Lapalme, 2012)
Enterprise Ecological Adaptation (EEA)	EA is the means for organizational innovation and sustainability. The organization is designed, including its relationship to the environment. The enterprise and environment are co-evolving. (Korhonen et al., 2016; Lapalme, 2012)

For this research, I adopt the definition of EA from ISO 42010. This definition looks at the enterprise in its environment, including influences and external effects (ISO, 2022c). This definition fits the EEA school of thought as defined by Lapalme (2012).

2.4.3 Enterprise Architecture Concepts

EA can provide a holistic view of the enterprise (Jonkers et al., 2006; Korhonen et al., 2016) and is often seen as a comprehensive 'blueprint', covering Business, Data, Application, and Technology domains (Kotusev, 2018; Kotusev et al., 2022; The Open Group, 2022c). Kotusev et al. (2017) include Security as a fifth domain in EA, while TOGAF describes Security as a 'cross-cutting concern' by combining appropriate views of the Business, Data, Application, and Technology domains (The Open Group, 2022c), see Figure 6.

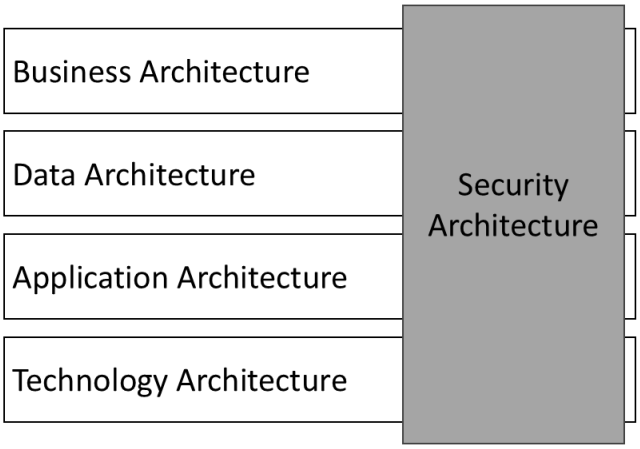

Figure 6. Security Architecture as a Cross-cutting Concern in EA

Villalón-Fonseca (2022) argues that CS can be effectively managed with an architecture-based approach, especially if the architecture combines the following viewpoints:

1) The system viewpoint, for describing the system, including its components and relationships, which needs to be secured;
2) The security viewpoint, for describing the security requirements and concerns, usually derived from a risk assessment or other security-related criteria;
3) The process viewpoint, for establishing a methodology to define and implement a set of security controls to make the system more secure, in line with its security objectives.

The viewpoints and concerns differ per stakeholder, as not every stakeholder has the same view and/or viewpoint on a system (ISO, 2022c; Lankhorst, 2017; The Open Group, 2022b). For example, the Chief Information Security Officer (CISO) would look differently to the implementation of a new HR application than the Chief Financial Officer (CFO) (Lankhorst, 2017). An EA is usually composed of multiple individual documents called EA artifacts that describe the different views and viewpoints of stakeholders. Examples of EA artifacts are Principles, Policies, Standards, Guidelines, and Reference Architectures (Kotusev et al., 2022; Kurnia et al., 2020).

2.4.4 Enterprise Architecture Frameworks

As briefly discussed in section 2.3.2, the current concept of EA is defined by popular EA frameworks (EAFs) such as The Zachman Framework and TOGAF (Kotusev, 2018). Although these frameworks provide high-level EA implementation guidance (Jonkers et al., 2006), none of the frameworks can be used without critical modifications (Kotusev, 2018; Molnar & Proper, 2013).

As a response to traditional EA Frameworks such as TOGAF, Agile EAFs are on the rise (Kotusev, 2020; Van Wessel et al., 2023). Agile EAFs, such as The Open Groups' Open Agile Architecture (O-AA), are more modular than its traditional counterparts and follow short, rapid cycles to continuously deliver value to stakeholders (The Open Group, 2022b). Security is embedded in agile architectures through software development practices, such as DevSecOps, Threat Modelling and Security by Design, which help enable the agile architecture to meet quality and security standards (Becks, 2024; The Open Group, 2022c).

2.4.5 Enterprise Security Architecture Frameworks

In addition to traditional EAFs, there are frameworks that are predominantly focused on Security. These are called Enterprise Security Architecture Frameworks (ESAFs) (Diefenbach et al., 2019). Examples of ESAFs are Gartner's Enterprise Information Security Architecture (EISA) (Scholtz, 2006) and the Sherwood Applied Business Security Architecture (SABSA) (Burkett, 2012; Sherwood et al., 2005). SABSA is the most common used framework with practical contributions documented in numerous publications (see e.g., Al-Turkistani et al., 2021; Pöhn et al., 2023). The SABSA model consists of six layers that are closely related to an EAF such as TOGAF, see Figure 7 (Burkett, 2012). Each layer represents the view of a different stakeholder in the process of specifying, designing, constructing, and using the Security Architecture (Sherwood et al., 2005).

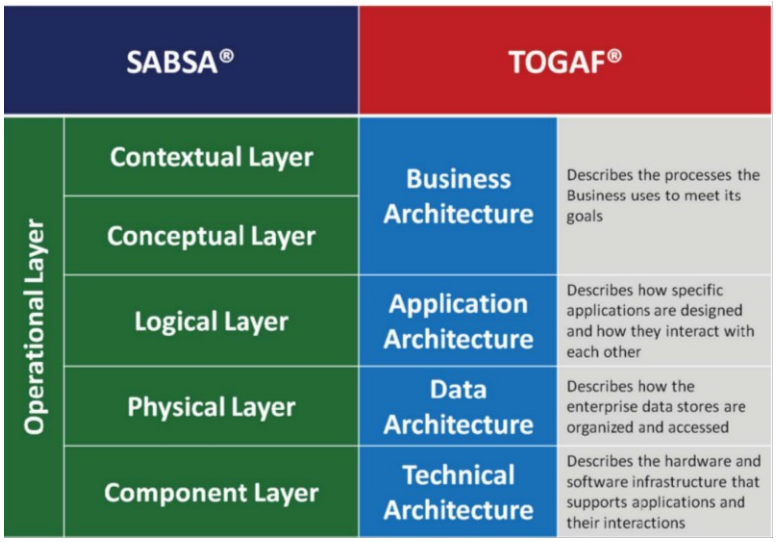

Figure 7. The SABSA Model and Layers (Burkett, 2012)

TOGAF has also introduced an extension of its framework with security-related aspects that are closely linked to SABSA, with the goal of taking the TOGAF standard to a higher conceptual level (The Open Group, 2022a). Integrating Security Architecture with EA is beneficial because Security Architecture builds on existing enterprise information and, in turn, influences the EA. Therefore, it is crucial for Security Architects and Enterprise Architects to speak the same language (The Open Group, 2022a). The Open Group has extended the TOGAF Architecture Development Method (ADM) with security and risk-related artifacts, see Figure 8. For example, in the preliminary phase of the ADM, *security principles, risk appetite* and *business impact* are defined artifacts to establish the context required to guide security architecture design (The Open Group, 2022a).

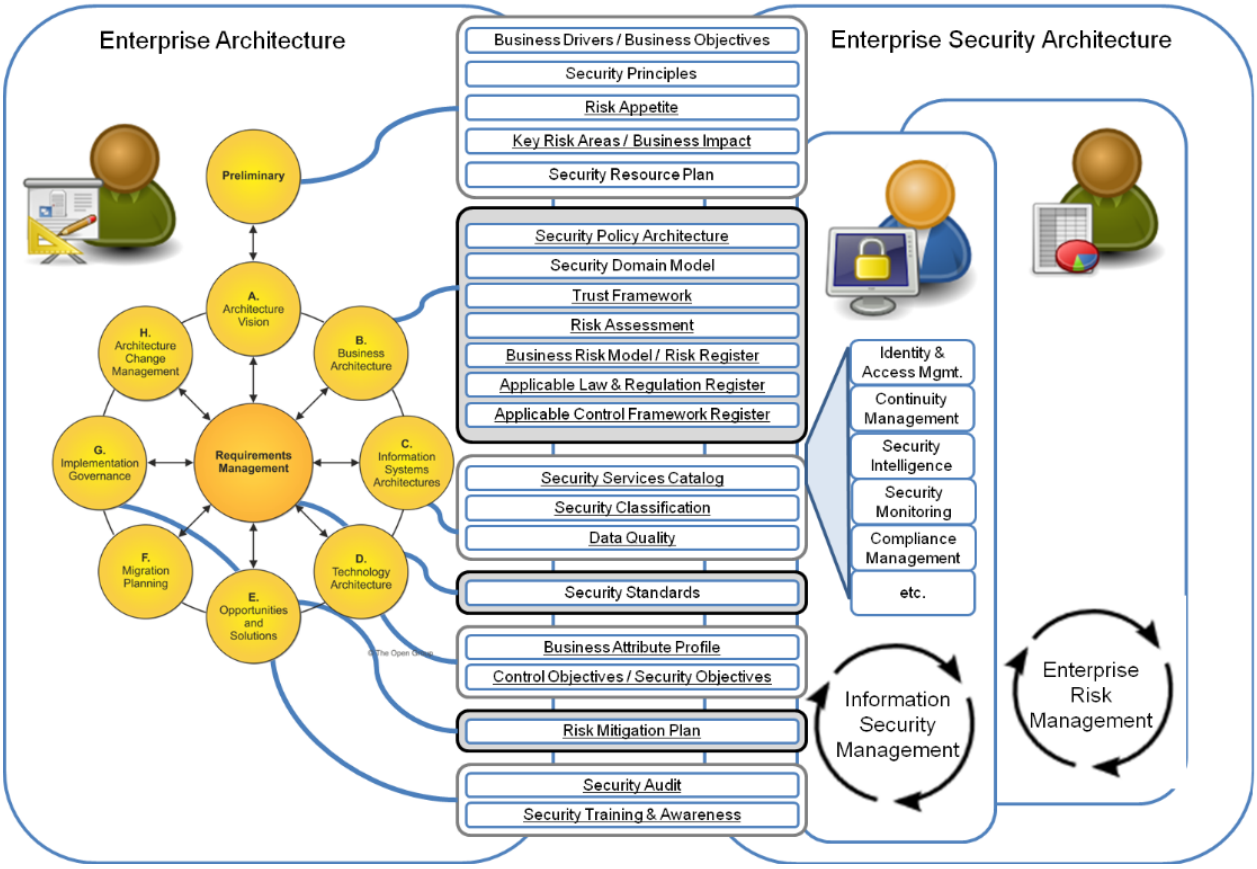

Figure 8. Security and Risk Concepts mapped to the TOGAF ADM (The Open Group, 2022a)

Research has identified a significant challenge in modeling CS within EA (Jiang et al., 2024; Mayer et al., 2019; Oliveira et al., 2022). This challenge persists even when using ArchiMate, the default modelling language from The Open Group. Although Band et al. (2019) have proposed ways to incorporate security and risk viewpoints into ArchiMate, these approaches still face issues related to standardization, complexity, and completeness (Jiang et al., 2024). As a result, it is challenging for stakeholders to effectively model and consider security requirements (Jiang et al., 2024; Oliveira et al., 2022).

2.5 Cyber Risk Management

This section describes the concept of Cyber Risk Management (CRM), including an introduction to general Risk Management terminology, a taxonomy of cyber risks and the CRM process used in this research.

2.5.1 Introduction to Risk and Risk Management

Before the concept of cyber risk is introduced, it is convenient to start with general Risk Management terminology. In section 2.3.3, I briefly introduced the risk components of 'probability' and 'impact.' In the most simplistic way, risk can be determined by the below formula (Refsdal et al., 2015):

Risk = Probability X Impact.

Refsdal et al. (2015, p. 9) define risk as "*The potential that something goes wrong and thereby causes harm or loss."* The International Standardization Organization (ISO, 2018, p. 1) defines risk as "*effect of uncertainty on objectives*." These definitions express the same idea, by adding the uncertainty dimension to adverse events and their consequences (Aven, 2016; Refsdal et al., 2015). Most organizations implement some form of Risk Management to manage potential risks (Refsdal et al., 2015; Stine et al., 2020). Risk Management involves the *"coordinated activities to direct and control an organization with regard to risk"* (ISO, 2018, p. 1). Examples of well-known Risk Management frameworks are ISO 31000 (ISO, 2018) and the Committee of Sponsoring Organizations (COSO) ERM framework (Barateiro et al., 2012; Efe, 2023).

2.5.2 Cyber Risk Management within Enterprise Risk Management

Cyber risk is one example of the broad array of risks that enterprises face. Cyber risk is classified as an operational risk within Enterprise Risk Management (ERM) theory, see Figure 9 (Cebula et al., 2010; Eling et al., 2021; Francis, 2019; Stine et al., 2020). Operational risk can be defined as "*The risk of loss resulting from inadequate or failed processes, people and systems or from external events*." (Francis, 2019, p. 6). Placing cyber risk among operational risk has gained widespread acceptance in research and practice (Eling et al., 2021; Strupczewski, 2021).

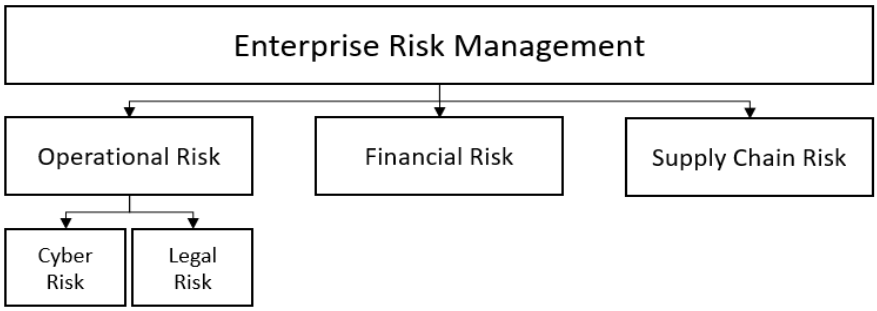

Figure 9. Cyber Risk as an Operational Risk in Enterprise Risk Management

2.5.3 Defining Cyber Risk Management

Drawing from a Literature Review on the definitions of cyber risk, Strupczewski (2021, p. 6) defines cyber risk as "*An operational risk associated with the performance of activities in cyberspace, threatening information assets, ICT resources and technological assets, which may cause material damage to tangible and intangible assets of an organization.*" This definition is in line with the classification of cyber risk as an operational risk as initiated by Cebula et al. (2010), see Figure 9, and the definition of Cyber Security as defined by Von Solms and Van Niekerk (2013) and Eling et al. (2021), see section 2.2.2. This is relevant because, although academic work on CRM is relatively young, there is some consensus on how the core concepts are defined (Eling et al., 2021; Strupczewski, 2021). The definition provided by Strupczewski (2021, p. 6) will be used going forward.

As discussed in section 2.5.2, cyber risk differs from conventional risk, although there is some overlap between the two. Böhme et al. (2018) differentiate between two key components: risk arrival, which refers to the processes leading to loss events (the 'probability' of an event), and the risk target, which encompasses the assets impacted by these loss events (the 'impact'). Both elements can fall under either the cyber or conventional risk domains, as illustrated in Table 4 (Böhme et al., 2019).

Table 4. *Distinction Between Cyber and Conventional Risk (adopted from Böhme et al., 2018)*

No.	Loss event	Risk arrival domain	Risk target domain
1	A Ransomware attack encrypts servers used by the Human Resources (HR) department	Cyber	Cyber
2	An earthquake destroys a data center	Conventional	Cyber
3	A DDoS-attack against an airport disrupts and delays air traffic	Cyber	Conventional

Cebula et al. (2010) have proposed an 'Operational Cyber Risk' taxonomy, which divides cyber risk into four categories:

1. **Actions of people**: Action, or lack of action, taken by people either deliberately or accidentally that impacts CS;
2. **Systems and technology failures:** Failure of hardware, software, and information systems;
3. **Failed internal processes:** failures in the internal business processes that impact the ability to implement, manage, and sustain CS;
4. **External events:** Issues often outside the control of the organization, such as disasters, legal issues, and supply chain risks.

To summarize, cyber risk is an operational risk that is located in cyberspace, which can impact both the virtual and physical world (Böhme et al., 2019; Cebula et al., 2010; Strupczewski, 2021).

2.5.4 Cyber Risk Management Frameworks

To manage cyber risks, enterprises usually adopt some kind of Risk Management approach (Diefenbach et al., 2019; Eling et al., 2021). The ISO employs multiple Risk Management frameworks, such as the ISO 31000 standard on Risk Management and ISO 27005 for Information- and Cyber Security Risk Management (ISO, 2022b). Both frameworks follow the same process and underscore the importance of integrating the framework with the enterprise's goals and objectives (Efe, 2023; ISO, 2018, 2022b). Eling et al. (2021) propose a CRM framework that is based on ISO 31000 and ISO 27005 but with a specific focus on cyber risk, see Table 5.

Table 5. *Cyber Risk Management (CRM) Process (adopted from: Eling et al., 2021)*

Process	Description
Context Establishment	Understanding the organizational environment, identifying the factors that can influence cyber risks, and defining the parameters for managing risks, such as the risk appetite (ISO, 2022b; Refsdal et al., 2015).
Risk Identification	The process to gather, recognize and describe cyber risks (ISO, 2022b), including gaining insights into incidents that might occur and cause potential harm to organizational assets (Refsdal et al., 2015).
Risk Analysis	Determining the level of cyber risk, typically in terms of the probability of occurrence and the impact on assets. This can be done qualitatively or quantitatively (ISO, 2022b; Refsdal et al., 2015).
Risk Evaluation	Determining whether the cyber risk and its significance is acceptable and to prioritize unacceptable cyber risks for Risk Treatment (ISO, 2022b; Refsdal et al., 2015).
Risk Treatment	Deciding on strategies and controls to deal with cyber risks. Treatments can interact and multiple treatments can be applied (Eling et al., 2021). There are four strategies: 1. Risk Acceptance - the informed decision to take (or accept) a particular risk (ISO, 2022b); 2. Risk Avoidance – avoiding a risk altogether, by not engaging in the activity (Refsdal et al., 2015); 3. Risk Mitigation – The process to modify risk by removing the risk *source,* changing the *probability,* and/or changing the *impact* (ISO, 2022a); 4. Risk Transfer – agreed distribution of risk with other parties, e.g., through cyber insurance (Eling et al., 2021; ISO, 2022a).

Understanding the different steps of the CRM process is important because integrating CS and EA can contribute to improved CRM in more than one step of this process (Diefenbach et al., 2019; Eling et al., 2021). My research tries to identify what the impact of the integration of CS and EA is on CRM, by looking at all steps of the CRM process as described in Table 5.

2.6 Integrating Cyber Security and Enterprise Architecture

Although both Cyber Security (CS) and Enterprise Architecture (EA) are novel scientific fields, there is prior research on the integration of the two concepts, as I described in the Theoretical Background (see chapter 2). Many of the identified publications focused on 'why' CS and EA should be integrated and do not make clear 'how' that integration should look like. To summarize the findings, I have created an overview that is divided into two categories:

1. Benefits ('Why' CS and EA should be integrated);
2. Strategies ('How' CS and EA could be integrated).

2.6.1 Benefits for Integrating Cyber Security and Enterprise Architecture

This section describes the benefits for integrating CS and EA within enterprises. Table 6 describes the benefits derived from the Literature Review:

Table 6. *Benefits for Integrating CS and EA*

Benefit	Description
Identification of Assets	EA facilitates the identification of primary assets, such as business processes and information, as well as secondary assets, including hardware, software, and networking components. This comprehensive asset inventory is advantageous for both CS and Risk Management (Diefenbach et al., 2019).
Enhanced Information Sharing	Promoting the exchange of information between CS and EA teams improves collaboration and understanding (Loft et al., 2021).
Common Language for Cyber Risk Management	Establishing a common language for managing cyber risk enables clearer communication and more effective strategies between CS and EA practitioners (Oda et al., 2009; Scholtz, 2006)
Integrated Risk Assessment	Integrating risk assessments across multiple levels—enterprise, domain, system, and component—strengthens the overall risk management approach within the enterprise (Loft et al., 2021; Pulkkinen et al., 2007; Ruan, 2019).
Improved Incident Response	Integrating CS and EA activities will allow enterprises to act immediately during and after security incidents (Al-Turkistani et al., 2021);
Reduction of Business Risks	Integrating CS and EA can lead to reduced business risks, increased disaster tolerance, and a reduction in security breaches (Ross et al., 2006).

These benefits make it clear that EA is indeed a promising vehicle to manage CS and can therefore contribute to making enterprises more resilient against cyber risks (Al-Turkistani et al., 2021; Diefenbach et al., 2019; Eling et al., 2021).

2.6.2 Strategies for Integrating Cyber Security and Enterprise Architecture

This section describes strategies that enterprises can adopt to effectively integrate CS and EA as identified in the Literature Review. A key contribution to this field is the work of Diefenbach et al. (2019), who provide a comprehensive mapping of the concepts related to Information Security Management (ISM), Risk Management (RM), and EA. Their analysis uses widely recognized frameworks, including ISO 27001, ISO 27005, ISO 31000, and ISO 42010, as illustrated in Figure 10.

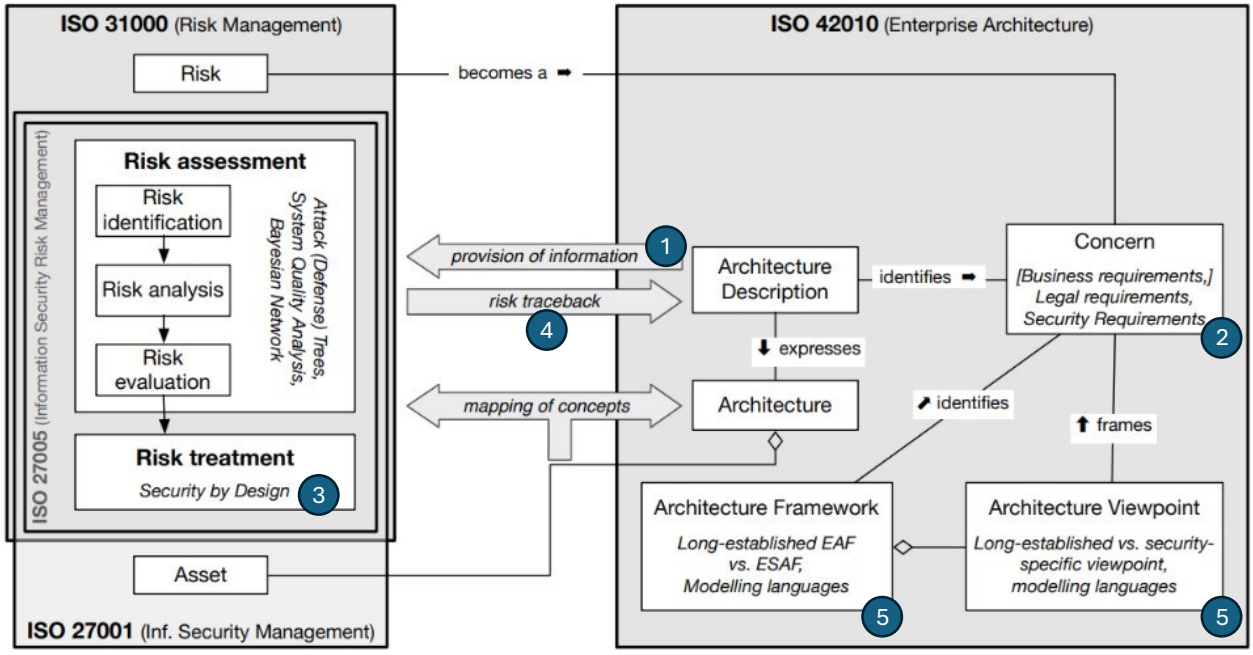

Figure 10. Integration of ISO 27001, ISO 31000, and ISO 42010 (Diefenbach et al., 2019)

This model illustrates the interrelationships among the concepts outlined in the referenced ISO standards. For example, in the context of ISO 27001, an asset plays a crucial role in providing architecture-related information and can be represented through elements of an Enterprise Architecture Description (EAD), a concept defined in ISO 42010 (Diefenbach et al., 2019). The EAD can in turn be used to provide input for Risk Assessment, which is an element described by ISO 31000 and ISO 27005 (Diefenbach et al., 2019). Additionally, the principle of Security by Design is highlighted as a method of Risk Treatment to manage cyber risks effectively. This principle can be integrated into EA to ensure the secure design of information systems throughout their lifecycle (Loft et al., 2022; Mees, 2017). It is therefore important to recognize the interrelationships among the concepts of EA, CS, and Risk Management, as illustrated by the arrows in Figure 10.

The conceptual mapping presented by Diefenbach et al. (2019) in Figure 10 provides essential input for the Focus Groups and interviews conducted in this research. The associated strategies for

integrating CS and EA are derived from this framework and are detailed in Table 7. It is crucial to note that these strategies are interconnected and should not be considered in isolation (Diefenbach et al., 2019). The strategy of "Aligning Business & IT Activities," identified as number 6, is the only one not included by Diefenbach et al. (2019). This strategy, drawn from the works of Jarjoui & Murimi (2021) and Kotusev (2018), serves as a cohesive element that integrates the other strategies. The strategies numbered 1 through 5 in Figure 10 correspond to their respective entries in Table 7.

Table 7. *Strategies for Integrating Cyber Security and Enterprise Architecture*

No.	Strategy	Description
1	EA providing input information for cyber risk assessment	EA can provide valuable input information for cyber risk assessments by employing EA Descriptions (EADs) (Diefenbach et al., 2019).
2	Integrating security requirements with other requirements	Security-related aspects should be considered during the Requirements Engineering (RE) phase of EA by integrating security requirements with other critical requirements, such as business or legal requirements (Diefenbach et al., 2019; Niemi & Pekkola, 2020).
3	Adopting the 'Security by Design' paradigm	Implementing the 'Security by Design' approach allows developers to address security considerations from the beginning of an EA asset's lifecycle (Diefenbach et al., 2019; Mees, 2017).
4	Providing a risk traceback to EA assets	Cyber Risk Management should establish a risk traceback mechanism to EA assets, rather than documenting risk decisions in isolated risk registers outside of EA (Diefenbach et al., 2019).
5	Integrating Cyber Security into EA frameworks	EA Frameworks should be extended to include CS viewpoints, stakeholder perspectives, and concerns (Diefenbach et al., 2019; Loft et al., 2022; Mayer et al., 2019; Niemi & Pekkola, 2020).
6	Aligning Business & IT Activities	Coordinating and streamlining organizational efforts to address cyber risks can be facilitated by aligning Business and IT activities (Jarjoui & Murimi, 2021).

Based on a comprehensive review of relevant literature, six key strategies for integrating CS and EA are described in Table 7. These strategies will be presented to the Focus Group and interview participants to gather qualitative feedback and to assess their perceived importance in practice.

3 Research Methods

This chapter outlines the research methodology, data collection, and analysis methods employed in this study. It also addresses the quality of the research and the ethical considerations that guided the process.

3.1 Research Methodology

This research adopts a qualitative, naturalistic approach, aimed at exploring various phenomena within social contexts. It emphasizes the description of individuals and their interactions in naturally occurring settings (Bell et al., 2022; Recker, 2021). I follow the main steps of qualitative research as described by Bell et al. (2022), illustrated in Figure 11.

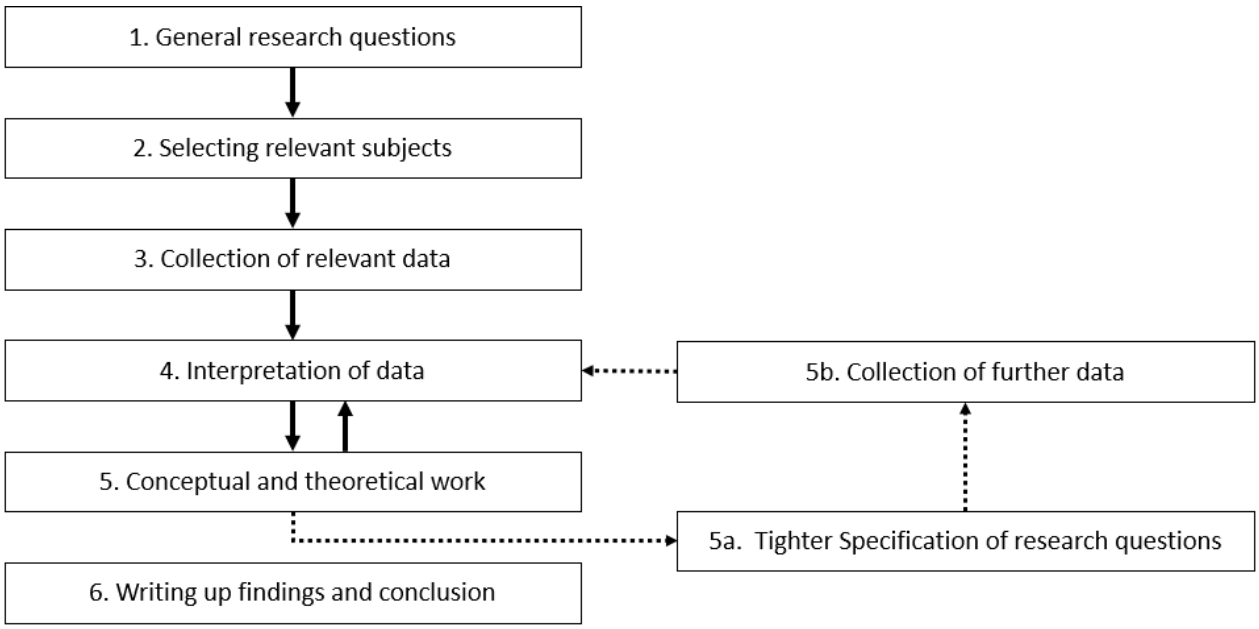

Figure 11. Outline of the Main Steps of Qualitative Research (Bell et al., 2022)

Initially, I formulated a general Research Question (RQ) focused on the integration of Cyber Security (CS) and Enterprise Architecture (EA) and the impact on Cyber Risk Management (CRM). Next, I selected participants with a strong familiarity with these concepts who could meaningfully contribute to the construction of knowledge. Empirical data was collected through a Focus Group and four expert interviews.

After the collection of data, I employed thematic analysis, utilizing open and axial coding (as detailed in section 5.5) to analyze and interpret the findings. During this process, I was under supervision to ensure a rigorous process was followed and decisions were documented correctly. Finally, I wrote up the findings and discussion of my research, see Chapter 4 and 5.

For this research, I opted for a combination of exploratory and explanatory research methodologies, because existing knowledge regarding the integration of CS and EA, particularly in relation to CRM, is scant (Diefenbach et al., 2019; Eling et al., 2021). Qualitative research is particularly suitable for exploratory studies, especially when the phenomenon under investigation is not fully understood, insufficiently researched, or still emerging (Recker, 2021). The aim of this study is to identify strategies that enterprises can use to integrate CS and EA, and to evaluate how this integration impacts CRM. Figure 12 illustrates the positioning of this research on the exploratory-explanatory continuum as described by Recker (2021).

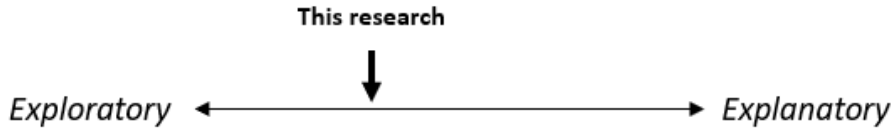

Figure 12. This Research Situated on the Exploratory-Explanatory Continuum

3.2 Research Strategy

This research employs a combination of deduction, induction, and abduction to construct meaning. Deduction can be defined as "*a form of logical reasoning that involves deriving arguments logically from general premises to specific instances. It is used to test hypotheses and propositions*" (Recker, 2021, p. 42). This approach is utilized in my study to evaluate the model proposed by Diefenbach et al. (2019) by asking both Focus Group and interview participants to rank the perceived importance of the strategies and identify any missing elements.

In contrast, induction "*infers general conclusions from specific observations, forming hypotheses and theories by identifying patterns. It is about deriving theoretical concepts from observed data, moving from specifics to generalities to generate new knowledge*" (Recker, 2021, p. 42). Through the qualitative data collected from the Focus Groups and interviews, I have generated novel insights into the integration of CS and EA and their effects on CRM.

Finally, abduction is described as "*the process of making sense of an observation by drawing inferences about the best possible explanation through trial-and-error, often termed as 'educated guessing.' Abduction is distinct from inference or deduction because it focuses on finding satisfactory explanations for observed consequences*" (Recker, 2021, p. 42). In my research, this process is employed to synthesize the findings from participants and derive explanations for the integration strategies that emerged.

Combining these three strategies allowed me to gain an initial understanding of the phenomenon under study, make sense of the complexities involved, and validate my developed theories with experts and practitioners (Recker, 2021, p. 43). This process is visualized in Figure 13.

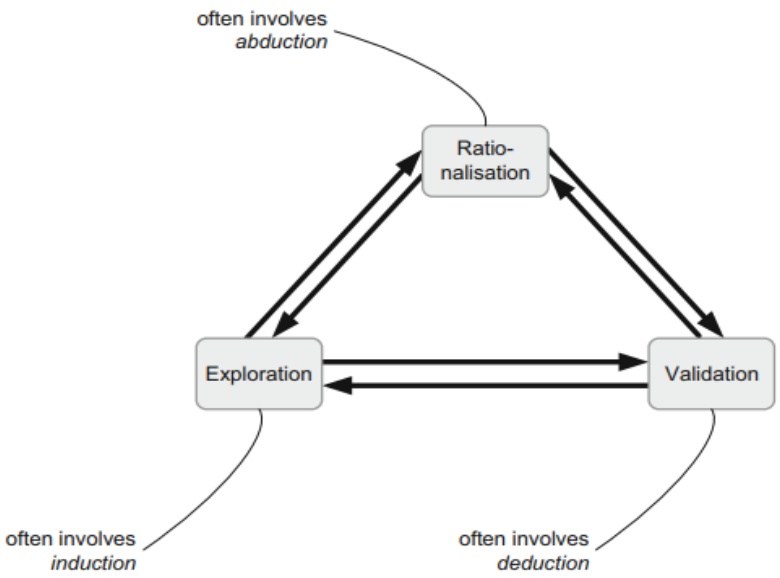

Figure 13. Deduction, Induction, and Abduction in Research Design (Recker, 2021)

The integration of CS and EA is an emerging topic often explored through qualitative strategies, which help identify and describe key concepts influencing this integration (Recker, 2021). However, qualitative research presents challenges, including difficulties in generalizing findings and issues with reliability and replicability due to contextual factors (Recker, 2021). To mitigate these limitations, this study employs triangulation, which involves using multiple sources of evidence about a phenomenon (Recker, 2021).

This research combines a Literature Review with a Focus Group and expert interviews to achieve triangulation, as illustrated in Figure 14 (Bell et al., 2022; Recker, 2021). The Focus Group encourages participant discussion, emphasizing group interaction and the construction of meaning (Bell et al., 2022; Bobbert & Mulder, 2013). Expert interviews serve as a means for cross-validation, allowing different data types and sources to converge on the phenomenon (Bell et al., 2022; Recker, 2021). Sections 3.3 and 3.4 detail the data collection and analysis methods for the Focus Groups and expert interviews.

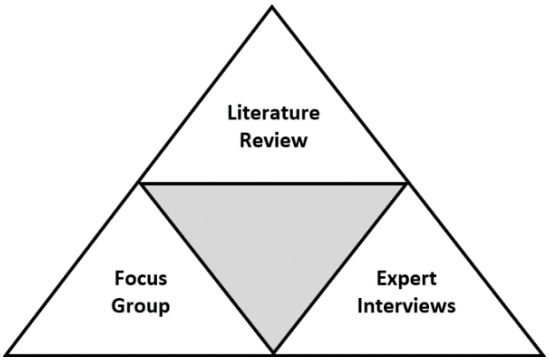

Figure 14. Triangulation Methods

3.3 Data Collection Methods

This section describes the data collection methods that I have used to collect theoretical and empirical data.

3.3.1 Literature Review

The Literature Review (LR) provides an overview of the current body of knowledge on Cyber Security (CS), Enterprise Architecture (EA), and Cyber Risk Management (CRM) and contributes to my understanding of how CS and EA can be integrated, including their impact on CRM.

Identification of Sources

The LR was conducted between September 2023 and April 2024 using the search library from the HU University of Applied Sciences (HUGO) and Google Scholar. These databases provided access to multiple sources, including ScienceDirect, SpringerLink, and Web of Science. Following an initial exploratory search on the core concepts, I developed a search strategy using specific queries to enhance replicability and transparency (Bell et al., 2022; Recker, 2021). Boolean (AND/OR) operators were applied to refine the search and reduce irrelevant results. The search queries are listed below:

- (“Enterprise Architecture”) AND (“Cyber Security” OR “cybersec*” OR “Information Security” OR “IT Security”) AND (“Integration” OR “Review” OR “Practices” OR “Factors” OR “Strateg*”);
- (“Enterprise Architecture”) AND (“Cyber Risk” OR “Cyber-Risk” OR “Cybersecurity Risk” OR “Information Security Risk” OR “IT Risk”).

Inclusion Criteria

Table 8 outlines the inclusion criteria applied to enhance the quality of the search, ensuring that only relevant and high-quality literature was selected for this research.

Table 8. *Inclusion Criteria*

No.	Criteria	Values for inclusion
1	Duplication	Non-duplicate articles
2	Language	English or Dutch
3	Sources	Scientific publications (preferably peer-reviewed)
4	Format	Publications with citations and references

Retrieval of Literature

After the search queries were reviewed by my supervisors, the search was executed. The relevancy of the articles was determined by reading the title and abstract (Bell et al., 2022). The primary focus of the LR was on peer reviewed articles, ensuring the use of reliable publications and allow for high quality research

(Bell et al., 2022). Non-peer reviewed articles were included as well if they were deemed valuable. Examples are reports from the International Organization for Standardization (ISO) and the National Institute for Standards and Technology (NIST), as well as publicly accessible framework documentation such as TOGAF and SABSA. These reports supplemented the literature search by providing insights in currently emerging topics and by describing well-known standards and frameworks (Bell et al., 2022).

Organizing Literature

All relevant publications that met the inclusion criteria were stored in Mendeley, a reference management software. Upon upload, the metadata of the publication was evaluated and, when necessary, edited to ensure the references were correct and up to date and in conformance with APA. The co-supervisor reviewed the remaining publications to ensure the use of high-quality publications.

Furthermore, several publications were recommended that did not appear in the original search. These publications were included after carefully reviewing the relevancy of the article in the context of this research. Examples of publications that were added but did not show up in the original search were articles behind a paywall, articles that were not accessible through HUGO and Google Scholar, and articles that used a different taxonomy than the one used in my developed search queries. The core publications that align with the search queries and criteria are listed in Appendix A. The literature search process is illustrated in Figure 15.

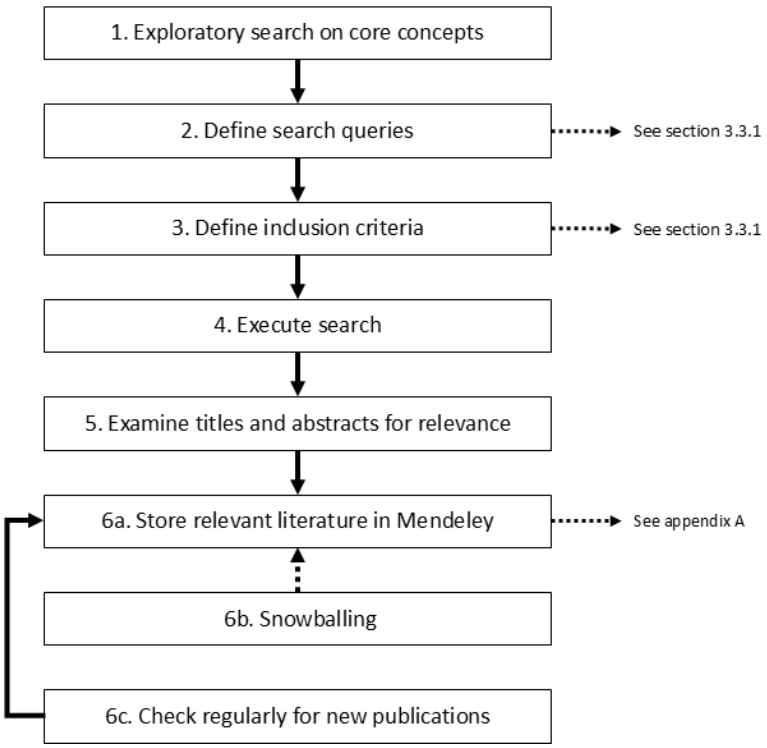

Figure 15. Literature Search Process

3.3.2 Focus Group

This research utilizes a Focus Group to gather empirical evidence on the integration of CS and EA. The Focus Group explores how experts and practitioners collectively understand this topic, emphasizing group interaction and construction of meaning, which is ideal for qualitative and explorative research (Bell et al., 2022).

Focus Group Participants

Purposive sampling was used to select participants based on their relevant knowledge and interest in CS and EA integration (Bell et al., 2022). The eligibility criteria for Focus Group participation were:

- Over five years of professional experience in roles related to CS and EA, such as Enterprise Architects, Domain Architects, Security Architects and CISOs;
- Fluency in Dutch;
- Signed informed consent, see section 5.3.1.

Based on the criteria, seven participants were invited to participate in the Focus Group, of which six eventually attended. The participants are listed in Table 9.

Table 9. *Focus Group Participants*

Identifier	Role	Experience	Sector
A1	Enterprise Architect	~20 years	Consultancy
A2	Director Security and Compliance	~25 years	ICT
A3	Domain Architect Security	~20 years	Banking
A4	Security Architect	~20 years	Consultancy
A5	Enterprise Architect	~20 years	Engineering
A6	Associate Professor Cyber Security	~35 years	Education

To facilitate and structure the Focus Group, a Group Support System (GSS) called Meetingwizard was used. GSS tools have proven effective in conducting scientific research, providing relevant and valid findings (Bobbert & Mulder, 2013; Klein et al., 2007). A GSS facilitates group interaction and enhances idea generation, while allowing for anonymity of participation, parallel communication, and group memory (Klein et al., 2007).

The Focus Group followed a structured approach using a set of pre-developed questions, which were uploaded to Meetingwizard and presented to the participants. These questions, listed in Appendix B, were derived from the Literature Review (Chapter 2) and aimed to gather the following insights:

- How CS and EA are currently integrated within enterprises based on participants' experiences;
- Blockers (strategies that negatively influence the integration of CS and EA) identified by participants;
- Enablers (strategies that positively influence the integration of CS and EA) identified by participants;
- The impact of CS and EA integration on CRM within enterprises;
- Ranking the six strategies identified by Diefenbach et al. (2019) and Jarjoui & Murimi (2021) in section 2.6.2 by having participants rank these strategies based on perceived importance and relevance;
- Identifying additional strategies not mentioned in the Literature Review by asking participants if anything was missing.

These questions provided a clear understanding of current CS and EA integration, the key blockers and enablers, the impact on CRM, and helped prioritize relevant strategies for integrating CS and EA based on both literature and empirical data.

3.3.3 Interviews

For the expert interviews, four participants were selected using the same criteria applied for the Focus Group (see section 3.2.3). The interviews aimed to triangulate data and cross-validate the findings from the Focus Group (Recker, 2021). The goal was to reach theoretical saturation, meaning that no new or relevant data is emerging regarding the integration of CS and EA as phenomenon under study (Bell et al., 2022).

I conducted interviews with four participants, one of whom also participated in the Focus Group. This approach allowed the interviewee to elaborate on their perspectives in an anonymous setting, as participants may be hesitant to speak freely during Focus Groups (Bell et al., 2022). The interview participants are listed in Table 10.

Table 10. *Interview Participants*

Identifier	Role	Experience	Sector
B1	Enterprise Security Architect	~30 years	Telecommunications
B2	Domain Architect Security	~20 years	Banking
B3	Chief Information Security Officer	~25 years	Aviation
B4	Enterprise Architect	~15 years	Education

A semi-structured interview approach was adopted, using the same set of questions from the Focus Group to ensure consistency while allowing flexibility in responses (Bell et al., 2022). This method offers several advantages for my research. Firstly, it allows for adaptability, enabling me to modify questions based on participant responses for deeper insights. Secondly, this approach allowed me to have a more

natural conversation, encouraging participants to share their viewpoints more openly (Bell et al., 2022). An interview guide was developed to structure the interview process, which can be found in Appendix C.

All interviews were conducted via Microsoft Teams to facilitate the challenging schedules of the participants. When starting the session, I asked permission to record the interview, as outlined in the informed consent form (see section 3.6.1). Microsoft Teams produced a transcript of the interview, reducing the need for manual transcription (Bell et al., 2022). The transcript was reviewed, and minor adjustments were made, for example when a participant used the English word '*Cyber Security'* and the Dutch word '*cyberbeveiliging'* interchangeably. The interviews were produced verbatim, meaning that tics, stuttering, and hesitations are part of the interview transcript (Bell et al., 2022). The reason to choose for this transcription method is to allow for full transcription of not only *what* was said during the interview, but also *how* it was said (Bell et al., 2022).

3.4 Data Analysis

To analyze the unstructured data from the Focus Group and interviews, I applied thematic analysis, a widely used method for examining qualitative data. Thematic analysis is defined as "*a method for identifying, analyzing, organizing, describing, and reporting themes found within a data set*" (Braun & Clarke, 2006, p. 6; Nowell et al., 2017, p. 2). I used ATLAS.TI, a qualitative data analysis software, to assist with the coding process. To structure the thematic analysis, I followed the step-by-step approach outlined by Nowell et al. (2017). This process consists of six stages, as illustrated in Figure 16 and detailed below. Step 6, which involves producing the report, is not included in this description, as it pertains to the thesis rather than the analysis itself.

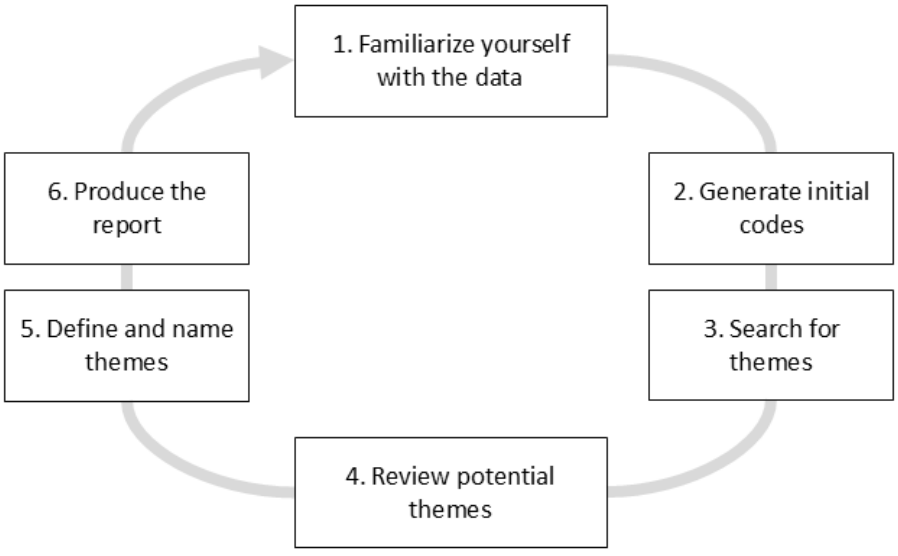

Figure 16. The Thematic Analysis Process (own work, based on Nowell et al., 2017)

1. **Familiarize yourself with the data**

I began by familiarizing myself with the data, a process facilitated by personally conducting and transcribing the interviews. This iterative process allowed me to engage deeply with the data from the start.

2. **Generate initial codes**

I then initiated the coding process, creating over 200 initial codes through open coding (Bell et al., 2022). This reflective process, supported by ATLAS.ti, helped organize the data systematically (Nowell et al., 2017). To enhance credibility, my co-supervisor reviewed the initial codes, ensuring accuracy through peer debriefing (Nowell et al., 2017).

3. **Search for themes**

Using axial coding (Bell et al., 2022), I organized initial codes into 'code groups' in ATLAS.ti, generating themes inductively. Thematic analysis allowed flexibility in theme creation, leading to key themes like blockers and enablers related to the integration of CS and EA (Nowell et al., 2017). During this process, several codes were renamed or changed to better reflect the emerging themes (Braun & Clarke, 2006; Nowell et al., 2017).

4. **Review potential themes**

After open and axial coding was completed, the co-supervisor reviewed the themes for validity, ensuring they accurately reflected the data. Based on this feedback, I refined the themes and developed the final list of categories presented in Chapter 4.

5. **Define and name themes**

Finally, I identified the narrative each theme represents and its relevance to the research questions, ensuring the themes were coherent and aligned with the participants' input (Braun & Clarke, 2006; Nowell et al., 2017).

3.5 Research Quality

This section describes the quality criteria of reliability and validity applied in this research to enhance the credibility of the findings.

3.5.1 Reliability

Reliability in qualitative research refers to the consistency and repeatability of the research process and results (Bell et al., 2022). To enhance the reliability of this study, I followed a systematic and transparent approach throughout the research process. First, I used clear and replicable data collection procedures, such as standardized interview guides for both the Focus Group and expert interviews. Additionally, I used

the qualitative data analysis software ATLAS.ti for the coding process, ensuring that data organization was consistent and traceable. To further improve reliability, I sought peer debriefing by having my co-supervisor review the initial codes and themes, allowing for feedback and refinement. This step helped to mitigate researcher bias and ensure consistency in the interpretation of data (Bell et al., 2022).

3.5.2 Validity

To enhance internal validity, I aligned data collection methods with the research questions, ensuring an in-depth exploration of the integration of CS and EA. Through inductive thematic analysis, I allowed themes to emerge from participants' responses, minimizing researcher bias. By using a GSS, I also made sure that statements from research participants were accurately captured and used in data analysis. Involving my co-supervisor in the review process provided additional validation, ensuring the findings were grounded in the data. For external validity, I selected participants from diverse professional backgrounds to capture a wide range of perspectives, improving the transferability of the findings to similar organizational contexts. Using multiple data sources, including a Focus Group and interviews with experts, enabled triangulation, which enhanced the validity of this research, see section 3.2 (Bell et al., 2022; Recker, 2021).

3.6 Ethical Considerations and Data Management

This section outlines the ethical considerations and data management practices implemented in this study. The Association for Information Systems (AIS) Code of Conduct was used in this study as a guideline for ethical research (Recker, 2021). In this section, I provide a more detailed explanation of five ethical principles that I applied in this research to mitigate ethical risks (Bell et al., 2022).

3.6.1 Informed Consent

Informed consent ensures that all participants receive and understand all the information they need to decide whether to take part in this research (Bell et al., 2022). To gather informed consent, a digital consent form was created and shared with participants. The informed consent form contained information about the research, such as an introduction, the goal and main Research Question. Every participant needed to consent to the form by choosing between 'agree or 'not agree' and submitting the form to the researcher for review. All participants provided their consent, confirming their voluntary participation. A copy of the Informed Consent Form can be found in Appendix D.

3.6.2 Minimization of Harm

Given that this research focuses on the intersection of CS and EA there is a potential risk that participants or their organizations could face negative consequences due to statements made about how CS is structured within those organizations (Macnish & Van der Ham, 2020). Therefore, in this research I adhere to the principle of 'minimization of harm', which ensures that no harm is intended and that any potential

harm to participants or non-participants, such as future users of the research, is minimized (Bell et al., 2022; Macnish & Van der Ham, 2020). To mitigate these risks, the following measures were implemented:

1. An informed consent form was used, guaranteeing voluntary participation, anonymity, and the right to opt-out at any stage (see section 3.5.1);
2. Any identifying information about participants or their organizations was masked, especially if the participant disclosed their employer's identity during the Focus Group or Interview, to ensure full anonymity.

3.6.3 Confidentiality

All data collected, processed, stored, and analyzed will be kept confidential and accessible only to individuals directly involved in this research. The data will not be shared with third parties unless required for the transparency and replicability of the study, in which case pseudonymization will be applied.

3.6.4 Privacy and Control of Data

Privacy and control of data are key concerns in CS research (Macnish & Van der Ham, 2020). To improve the privacy of research participants, participants will be pseudonymized, meaning that no information provided by participants is directly traceable to them. Furthermore, quotes that reveal the identity of the participant and/or the enterprise they represent will be masked to ensure anonymity. Consequently, only the minimum data necessary will be collected for the purpose of this research, following the principle of data minimization. In this case, any Personally Identifiable Information (PII), such as age, gender or religion will not be collected and analyzed, since this information does not provide any benefits to the outcome of this research (Macnish & Van der Ham, 2020). Finally, research participants have the right to be forgotten, meaning their data, or copies thereof, will be deleted upon request at any time. This option was outlined in the Informed Consent Form, see section 3.6.1 and Appendix D.

3.6.5 Using Generative Artificial Intelligence in This Research

Generative Artificial Intelligence (Gen AI) is increasingly being used in scientific research (Burger et al., 2023; Shopovski, 2024). In this research, ChatGPT from OpenAI was primarily used to review text and suggest revisions to enhance the readability and coherence of the thesis. I reviewed and edited the content as needed, and ensured no confidential data was shared with ChatGPT during the process. All findings and conclusions presented in this thesis are my own, as ChatGPT is unfit to suggest causality or draw novel research conclusions (Burger et al., 2023). Therefore, I take full responsibility of the content in this thesis, ensuring it aligns with standards for ethical research.

4 Findings

In this chapter, I present the findings from the Focus Group and interviews, structured around four sub-questions (SQ's). These questions explore the current integration of Cyber Security (CS) and Enterprise Architecture (EA) within enterprises, the blockers and enablers of this integration, and its impact on Cyber Risk Management. First, I examine how CS and EA are integrated in practice (SQ1). Next, I identify the key blockers that hinder integration (SQ2), followed by a discussion of the enablers that facilitate it (SQ3). Finally, I assess the impact of this integration on Cyber Risk Management (CRM) (SQ4).

4.1 Current Integration of Cyber Security and Enterprise Architecture

Theory implies that the integration of CS and EA has benefits for CRM within enterprises, see chapter 2. However, the practical level of integration and its facilitation in enterprises remained unclear.

4.1.1 Focus Group Results

To address this, participants in the Focus Group where asked: "*To what extent are Enterprise Architecture and Cyber Security integrated within enterprises based on your experience?"* Participants had the opportunity to answer the question based on a five-point Likert scale, with scores ranging from 1 (not integrated) to 5 (fully integrated). The participants answered with an average score of **3.2,** reflecting that CS and EA are currently '*somewhat integrated*,' see Table 11. Although there is a variance of 44%, no participant gave a score of either 1 or 5, which are the extremes on this scale. This means that participants perceive that there is some level of integration, while also suggesting room for improvement.

Table 11. *Current Integration of CS and EA within Enterprises According to Focus Group Participants*

Question	Answers (n=6)	Score	Variance
To what extent are Enterprise Architecture and Cyber Security integrated within enterprises based on your experience?	6	3.2	44%

Participants had the opportunity to comment on their answers. One of the participants mentioned that "*EA adds Cyber Security to projects as early as possible*" (Personal communication, 2024), indicating that CS is being incorporated into EA processes in an early stage. Another participant mentioned that "*EA and Security being different departments make a full integration between the two quite hard*" (Personal communication, 2024), pointing to a potential organizational barrier that is hindering integration.

Several participants highlighted the critical role of the CISO in facilitating the integration of CS and EA. One participant observed: "*The Enterprise Architect generally works closely with the CISO and security*

specialists at suppliers" (Personal communication, 2024). Another comment underscored the existence of some level of integration: "*The job title 'Security Architect' already implies that there is some level of integration between security and architecture*" (Personal communication, 2024). This comment was followed by approving sounds and gestures from all Focus Group participants.

4.1.2 Interview Results

In parallel with the Focus Group, experts were interviewed to understand their perspectives on the current integration of CS and EA within enterprises. Similar themes emerged, with participants underscoring organizational separation as a key challenge. One interviewee observed that "*What I often see is that there are still two separate parts within the organization, (…) where architecture is usually under the technical side of Enterprise Architecture, while Cyber Security is more aligned with its own branch, either under the CISO or Risk Management-related departments*" (Personal communication, 2024). This view was supported by another participant, who remarked that CS and EA *" are connected to each other, but not in a conscious or premeditated way*" (Personal communication, 2024), further emphasizing the lack of intentional coordination.

Another interview participant shared a more critical view, citing a negative experience where the connection between CS and EA was deliberately removed: *"They (management) have removed the connection between Information Security and Enterprise Architecture, and that leads to huge problems, because architects come up with something, but there's no cyber in it, and we come up with something, and it's difficult to agree with the architect on what should be done in terms of architecture"* (Personal communication, 2024). This highlights the consequences of an absent or poorly structured relationship between the two disciplines, where misalignment leads to operational difficulties and security gaps.

4.1.3 Prioritizing Strategies (Focus Group Only)

Following the assessment of current integration, Focus Group participants were asked to prioritize six strategies derived from the literature review, see section 2.6.2, based on their perceived importance to the integration of CS and EA. Participants were not only asked to allocate points to the presented strategies but were also encouraged to suggest additional strategies they considered missing. Interview participants were not asked to complete this prioritization exercise due to differences in the data collection methodology, as the Focus Group used a GSS to capture this data. The results in order of perceived importance are listed in Table 12.

Table 12. *Prioritizing Strategies by Focus Group participants*

Priority	Strategy	Score	Spread	Abstains
1	Integrating Cyber Security in EA frameworks	29.2	8%	0
2	Adopting the 'Security by Design' principle, so that developers can take security-related aspects into account at the beginning of an EA asset's lifecycle	25.8	12%	0
3	Integrating Business Requirements with Security Requirements	18.4	26%	0
4	EA can provide input information for cyber risk assessment.	15	18%	0
5	Cyber Risk Management can provide a risk traceback to EA assets	5.8	8%	0
6	Managing cyber risks by aligning business & IT activities	5.8	12%	0

The results indicate a clear prioritization of strategies for integrating CS and EA. The top two strategies, **Integrating Cyber Security in EA frameworks** (29.2%) and **Security by Design** (25.8%), account for over 55% of the total score, showing their perceived importance. The lower spread (8% and 12%) for these strategies suggests strong consensus among respondents. In contrast, **Integrating business with security requirements** (18.4%) and **EA providing input for cyber risk assessment** (15%) show a wider distribution, particularly the former with a 26% spread, indicating variability in its perceived importance. The two lowest-ranked strategies, both scoring 5.8%, demonstrate agreement on their relative insignificance, as evidenced by their minimal spread (8% and 12%). Finally, an addendum was suggested for the second factor, because **Security by Design** is not only related to developers, but in general applicable to "*enforce security to be part of the architecture*" (Personal communication, 2024). Participants agreed during discussions that this is due to the "*rise of modern software development and DevOps engineering, where security by design is common practice*" (Personal communication, 2024).

To extend the list of strategies derived from the Literature Review, Focus Group participants were asked to add additional strategies to the list that were deemed missing in their perspective. In total, eleven strategies were added, see Table 13.

Some strategies overlap with each other. For example: **DevSecOps - Security as an integral part of operations** (Number 1) closely aligns with **making security an explicit part of architecture** (Number 5). Furthermore, **Good security awareness in both the business and EA** (Number 2) shows similarities with **knowing and respecting each other's expertise (EA and CISO)** (Number 6). Finally, **Good security representation in the EA board** (Number 7) and **giving security, risk, privacy, and architecture a joint role in a board** (Number 11) both focus on ensuring security is embedded in organizational governance structures (Personal communication, 2024).

Table 13. *Additional Strategies Derived from the Focus Group (Personal communication, 2024)*

No.	Strategy
1	"DevSecOps - Security is an integral part of operations and changes."
2	"Good security awareness in both the business and EA. The CISO plays an important role in this."
3	"Have architects and security people within the organization engage in joint social activities. This fosters relationships that lead to more business connections."
4	"Separate the creation process into a phase of possibilities and a phase of limitations, after which you merge them."
5	"Make security an explicit part of architecture."
6	"Know each other's (EA and CISO) interests and respect each other's expertise."
7	"Good security representation in the EA board."
8	"Think about the architecture of security tooling/function."
9	"Iterations in your architecture deliverables, where you slowly but surely find the optimal balance."
10	"An impactful security incident."
11	"Give security, risk, privacy, and architecture a joint role in a board."

An interesting factor or practice that is distinct from others is: "*Have architects and security people within the organization engage in joint social activities. This fosters relationships that lead to more business connections*" (Personal communication, 2024). This highlights the potential for organizing social activities in addition to 'business activities' to foster collaboration and integration.

4.2 Blockers for the Integration of Cyber Security and Enterprise Architecture

To answer sub question 2: "*What are possible blockers for the integration of Enterprise Architecture and Cyber Security?",* both Focus Group and interview participants were asked to give strategies that negatively influence the level of integration between Cyber Security (CS) and Enterprise Architecture (EA) in enterprises based on their experience. Table 14 presents the key themes identified through the coding process, with a detailed explanation of each theme provided in sections 4.2.1 (Focus Group) and 4.2.2 (Interviews). The full list of individual codes that are associated with the themes in Table 14 can be found in Appendix E.

Table 14. *Overview of Key Themes Derived from Focus Group and Interview Results*

Focus Group	Interviews
Different Mindsets and Focus	Lack of Awareness and a Reactive Approach
Organizational Misalignment	Skills and Knowledge Gaps
Knowledge and Capacity Gaps	Process and Strategic Misalignment
Conflicting Interests	Technical Misalignment
	Organizational Structure

4.2.1 Focus Group Results

To understand why the integration between CS and EA is considered 'somewhat integrated,' as reflected by the score of 3.2, the Focus Group participants were asked: *"Why do you think EA and Cyber Security are not better integrated?"* In total, the participants gave 13 responses. Four key themes emerged:

1. **Different Mindsets and Focus**

A key theme discussed by participants was the different perspectives between CS and EA teams. EA professionals typically focus on business opportunities and possibilities, while CS teams prioritize risk mitigation. One participant described this contrast: "*Enterprise Architects think in possibilities, while Cyber Security thinks in limitations*" (Personal communication, 2024). Another added, "*EA prioritizes functional business needs, but the business doesn't adequately incorporate the risk perspective into their requirements*" (Personal communication, 2024).

Participants also noted that security is often involved too late in the process, as one participant pointed out, "*Architects are usually involved early in the process, but security comes in much later, which is wrong*" (Personal communication, 2024). This delay leads to security being treated "*as an afterthought*" (Personal communication, 2024). A third participants disagrees however, stating that "*EA adds cyber (security) as early as possible to projects"* (Personal communication, 2024).

2. **Organizational Misalignment**

The lack of established relationships and misaligned reporting structures between CS and EA teams hinder integration. Participants highlighted the importance of integrating both teams early in the decision-making process to avoid conflicts down the line. One participant explained: "*If you have two separate worlds with different visions, even if they are closely related, but you don't communicate much and have your own channels for alignment, eventually you will run into each other*" (Personal communication, 2024). Another emphasized, "*There are separate departments that only come together much higher in the hierarchy*" (Personal communication, 2024), suggesting that this lack of alignment results in decisions being made in isolation.

3. **Knowledge and Capacity Gaps**

Participants cited a lack of security expertise among EA professionals. As one participant explained: "*Enterprise Architects understand the move to the cloud, that's something they are working on, but the in-depth security knowledge required to understand the consequences of that move is missing*" (Personal communication, 2024). The overburdened nature of EA teams further exacerbates this issue, with security considerations often "forgotten" due to other pressing priorities. "*EA teams already have so much on their hands, which is why security is often forgotten. It is up to the security architect to break this cycle*" (Personal communication, 2024), one participant remarked.

4. **Conflicting Interests**

Lastly, participants highlighted how the different priorities and conflicting interests of CS and EA teams contribute to friction. One participant mentioned, "*There are conflicting interests between EA and Security,*" emphasizing how the divergent objectives of the two teams - one focusing on business functionality and the other on risk mitigation - create challenges for alignment (Personal communication, 2024). Another participant remarked on their differing perspectives, noting that "*there is a significant difference in focus between EA and Security*" which further complicates collaboration (Personal communication, 2024).

4.2.2 Interview Results

The analysis of the interview data revealed a total of 32 distinct blockers to the integration of CS and EA. The overarching themes are described below.

1. **Lack of Awareness and a Reactive Approach**

A recurring theme in the interviews was the reactive approach to security, with security teams often involved too late in the development process. One participant highlighted the importance of proactive involvement, stating: "*We (security) are very reactive, while we should be applying concepts like Secure by Design and identifying risks and threats proactively*" (Personal communication, 2024). Another interviewee echoed this sentiment, explaining: "*Part of the issue is that there isn't enough attention given upfront to what the actual threats and risks are, and the different drivers within the organization*" (Personal communication, 2024). Interviewees frequently pointed out that the distinct perspectives between CS and EA teams contribute to collaboration challenges. EA professionals often focus on functional business needs and opportunities, while CS teams prioritize risk mitigation, leading to siloed operations and security being seen as an afterthought.

2. **Skills and Knowledge Gaps**

Another recurring theme in the interviews was the lack of in-depth security expertise among EA professionals and vice versa (Personal communication, 2024). One participant stated: "*The enterprise architect doesn't have enough knowledge of the security measures that need to be implemented at the*

cybersecurity level" (Personal communication, 2024). Another elaborated: "*He (the enterprise architect) has cyber knowledge, but not in-depth knowledge. So, he does not fully understand what it means when certain things are included in the architecture*" (Personal communication, 2024).

3. Process and Strategic Misalignment

Participants also discussed how CS requirements are often excluded from EA processes and strategic planning. One interviewee remarked: "*Security measures that need to be implemented at the cybersecurity level are not well understood by others*" (Personal communication, 2024), illustrating the knowledge gap between CS and EA. This gap results in security considerations being sidelined, as they are not fully integrated into the strategic or technical planning of EA. Another participant mentioned, "*Enterprise Architects are focused on the business drivers, but they don't fully incorporate the risk perspective into their planning*" (Personal communication, 2024), reinforcing the idea that the misalignment between business goals and security needs remains a significant blocker.

4. Technical Misalignment

The interviews also revealed technical challenges in aligning CS and EA. Security risks are often overlooked until much later in the design process, creating gaps that are difficult to address once architecture plans are in motion (Personal communication, 2024). For instance, one participant shared: "*Enterprise Architects understand the business drivers, but when it comes to cybersecurity, the necessary security measures are not fully considered*" (Personal communication, 2024). This oversight is particularly pronounced in large technical projects, where the consequences of insufficient security planning can be severe.

5. Organizational Structure

The organizational disconnect between CS and EA was a major theme throughout the interviews. The lack of formal collaboration structures, combined with different reporting lines, hampers communication and coordination between teams. One interviewee summarized the issue: "*If you have two separate worlds with different visions, even if they are closely related, but you don't communicate much and have your own channels for alignment, eventually you will run into each other*" (Personal communication, 2024). Another added, "*The problem is that these departments only come together much later in the process, often resulting in disjointed decisions*" (Personal communication, 2024). This organizational divide continues to challenge the integration of CS and EA within enterprises.

4.2.3 Comparative Analysis of Focus Group and Interview data

There are clear parallels between the blockers identified in the Focus Group and those from the interviews. Both data sets underscore the structural and cultural misalignments that hinder integration, particularly around knowledge gaps and organizational silos.

For example, both the Focus Group's theme of **Knowledge and Capacity Gaps** and the interview theme of **Skills and Knowledge Gaps** emphasize the lack of expertise on both sides. The inability of EA professionals to integrate security early on due to a lack of knowledge seems to be a recurring issue, where in-depth security knowledge is especially missing (Personal communication, 2024).

Similarly, **Organizational Misalignment** in the Focus Group and **Organizational Structure** in the interviews both reflect how differing reporting structures and lack of cross-functional collaboration exacerbate these challenges. One interviewee highlighted this, saying: "*There are still two different worlds, two different visions*" (Personal communication, 2024).

Finally, **Conflicting Interests** from the Focus Group and **Cultural Differences and Mindset** from the interviews both point to the differences in culture between CS and EA teams. This divide creates misalignment in goals and priorities, making it difficult to achieve seamless integration. As one participant summarized: "*Enterprise Architecture focuses on developing business needs, Cyber Security focuses on risk mitigation*" (Personal communication, 2024).

These findings illustrate the systemic challenges that both Focus Group and interview participants experience, with common themes highlighting the need for better organizational alignment, communication, and cross-domain knowledge and expertise to improve the integration between CS and EA.

4.3 Enablers for the Integration of Cyber Security and Enterprise Architecture

To answer sub question 3: "*What are enablers for the integration of Enterprise Architecture and Cyber Security?",* both Focus Group and Interview participants were asked to give examples of strategies that positively influence the level of integration between Cyber Security (CS) and Enterprise Architecture (EA). Table 15 presents the key themes identified through the coding process, with a detailed explanation of each theme provided in sections 4.3.1 (Focus Group) and 4.3.2 (Interviews). The full list of individual codes that are associated with the themes in Table 15 can be found in Appendix F.

Table 15. Overview of Key Themes Derived from Focus Group and Interview Results

Focus Group	Interviews
Established EA Principles and Frameworks	Leadership and Strategic Alignment
Collaboration and Organizational Alignment	Collaboration and shared responsibility
Secure Development	Security Integration into EA Frameworks
Security as a Business Enabler	Security Awareness and Organizational Culture
Security Awareness and Knowledge	Holistic and Standardized Approaches

4.3.1 Focus Group Results

During the Focus Group, participants where asked *"Why do you think EA and Cyber Security are already somewhat integrated?"* Again, the participants gave 13 responses. The following key themes emerged:

1. **Established EA Principles and Frameworks**

Participants emphasized that "*security is embedded within EA through architecture principles*," suggesting that EA principles incorporate security aspects (Personal communication, 2024). Additionally, existing EA frameworks enhance the integration of security in EA by "*incorporating security within requirements management*" (Personal communication, 2024). Another participant remarked that "s*ecurity, risk management, compliancy, privacy, and business continuity management are capabilities that are included in the EA capability model*" (Personal communication, 2024).

2. **Collaboration and Organizational Alignment**

Integration is further supported by collaboration between EA and Security functions. For example, participants pointed to the role of the Chief Information Security Officer (CISO) in fostering this collaboration, stating, "*Integration is supported by collaboration between EA and Security functions, such as the CISO*" (Personal communication, 2024). One participant emphasized that "*security awareness within EA ensures that security is not neglected in architectural considerations*" (Personal communication, 2024).

3. **Secure Development**

The rise of secure development and agile methodologies has improved security integration within EA. Participants noted that these methodologies have made security considerations more common in development processes, with one stating, "*The rise of DevSecOps and Security by Design has made security integration more common"* (Personal communication, 2024).

4. **Security as a Business Enabler**

Subsequently, participants recognized that security is increasingly viewed as a business enabler rather than a constraint. One noted, "*The business recognizes that risk management and security are enablers of business goals*," illustrating a shift in mindset toward embracing security as part of the broader business strategy (Personal communication, 2024). Additionally, the acknowledgment of security as a distinct domain within architecture is important in achieving organizational objectives (Personal communication, 2024).

5. **Security Awareness and Knowledge**

Finally, participants acknowledged that knowledge of security at the EA level, called security awareness, is especially important. One participant stated: "*EA has a certain level of security awareness, which means security cannot be neglected.*" (Personal communication, 2024). Another participant agreed, remarking that currently "*EA already has some security knowledge"* (Personal communication, 2024).

4.3.2 Interview Results

The analysis of the interview data revealed a total of 35 distinct enablers to the integration of CS and EA. The overarching themes are described below.

1. **Leadership and Strategic Alignment**

One thing that is crucial for integrating EA and Cyber Security effectively according to one participant is "*Commitment from higher management*" (Personal communication, 2024). Other participants noted that senior management is actively engaged in this integration, with one even stating, "*The same manager should oversee EA and Cybersecurity*" to ensure a unified direction (Personal communication, 2024). A shared strategy between EA architects and the Chief Information Security Officer (CISO) further enhances alignment, as they are encouraged to "*follow the same strategy*" (Personal communication, 2024).

2. **Collaboration and Shared Responsibility**

Participants emphasized the importance of having cyber, architecture, and business representatives at the same table to "*speak each other's language*" (Personal communication, 2024), and "*facilitate joint document creation*" (Personal communication, 2024). This partnership between EA and security teams enables shared accountability, with the responsibility for security resting with autonomous DevOps teams. As one participant highlighted, "*The responsible person for products or services is accountable for security*,"

highlighting the importance of security being a shared responsibility rather than a siloed function (Personal communication, 2024). Another interviewee added that splitting responsibilities is crucial, by stating: "*the balance between splitting responsibilities across departments and then quickly coming back together in the hierarchy is, I think, crucial*" (Personal communication, 2024).

3. **Security Integration into EA Frameworks**

Better integration of security into EA frameworks is another critical enabler, as one participant noted that currently "*Security is embedded in EA frameworks*" (Personal communication, 2024). Participants mentioned that security should be modeled in EA, with security features included earlier in development processes. This integration not only ensures that security becomes a capability within EA but also aligns security requirements with business needs, facilitating a more holistic approach to architecture Security is embedded in EA frameworks (Personal communication, 2024).

4. **Security Awareness and Organizational Culture**

The interviews revealed that security awareness at the EA level is an enabler of the integration, with participants recognizing that "*there is more awareness among different organizational parts and teams that security is important and that we need to work on it*" (Personal communication, 2024). This heightened awareness includes the desire to make security measures and the integration "*more measurable*" (Personal communication, 2024).

5. **Holistic and Standardized Approaches**

A holistic approach to security is seen as essential for successful integration, as the Literature Review already pointed out, see chapter 2. Standardization in architecture is also vital, with security integrated at the process level instead of being an afterthought at the application level (Personal communication, 2024). One participant noted, "*If we make an effort early in the process to identify risks and directly implement security principles, and if everyone is aligned, then we've already identified the relationship between a potential risk and the product or asset*" (Personal communication, 2024).

4.3.3 Comparative Analysis of Focus Group and Interview Data

One thing that again stands out is that themes derived from the Focus Group are similar to themes derived from the interview data. both data sets highlight organizational alignment and collaboration, security awareness, and the embedding of security within EA frameworks as critical enablers for successful integration.

For example, the theme **Established EA Principles and Frameworks** from the Focus Group is related to the theme **Security Integration into EA Frameworks** from the interviews. One participant mentioned that through EA frameworks, Security by Design could be reached: "*If you have those (EA)*

frameworks in place and cybersecurity is part of them, then you basically have security by design" (Personal communication, 2024). Integrating security in EA frameworks also mitigates the risk of security being seen as an '*afterthought'* (Personal communication, 2024).

The problem however is that, according to another participant, there are not a lot of EA frameworks that incorporate security: "*There are few integrated frameworks at the moment that do that (Cyber Security, red.) well, I actually only know one: SABSA"* (Personal communication, 2024). This highlights the need for more suitable EA frameworks that integrate Security concepts.

4.4 Impact on Cyber Risk Management

The final question that needs to be answered is sub question 4: *What is the impact of the integration of Enterprise Architecture and Cyber Security on Cyber Risk Management?* By analyzing Focus Group and Interview data, the following findings have emerged.

4.4.1 Focus Group Results

There is consensus from the Focus Group participants that integrating CS and EA will lead to improved CRM. One participant mentioned: *"Mitigating measures are incorporated into the architecture, resulting in a coherent approach to (cyber) risk management"* (Personal communication, 2024). Another participant adds: *"Security is better embedded in architecture, resulting in fewer risks occurring"* (Personal communication, 2024), highlighting that CRM will improve in general when CS and EA are well integrated.

There was one participant who mentioned that the integration of CS and EA will complicate CRM efforts, *"because various perspectives need to be aligned (and who does that?)"* (Personal communication, 2024). After a group discussion on this statement, the participant mentioned that this will only be the case *"when there is no formal integration"* of CS and EA (Personal communication, 2024), highlighting that if CS and EA are integrated, CRM will improve as well.

4.4.2 Interview Results

After analyzing the interview results, it became clear that participants agreed that integrating CS and EA improves CRM. One participant mentions that CRM will become *"More efficient, faster, and more decisive"* (Personal communication, 2024). Another participant observed improvement across different steps of the CRM process, by stating "*I think that if you have integrated it well, you are better able to shape cyber risk management, actually assess your risks, and respond to them*" (Personal communication, 2024). Finally, a third interviewee foresees improvement in the Risk Identification phase, remarking: "*I think it reasonably helps in identifying and mapping out what kind of risks are actually involved, especially on the process level instead of the application level*" (Personal communication, 2024).

4.4.3 Mapping Improvements to the Cyber Risk Management Process

A novel finding of this research is that integrating CS and EA improves CRM in every step of the process. To ensure these improvements are included in this research, I mapped the data from both the Focus Group and Interviews to the CRM process steps outlined by Eling et al. (2021). The full list of individual codes mapped to the steps of the CRM process can be found in Appendix G.

Cyber Risk Management process steps:

1. Context Establishment
2. Risk Identification
3. Risk Analysis and Evaluation
4. Risk Treatment (accept, avoid, transfer, mitigate)
5. Monitoring and Review

Context Establishment

Several improvements have been observed by interviewees in the first step of the CRM process, Context Establishment. One participant mentioned that integrating CS and EA leads to improved Context Establishment because there is more *"Knowledge about processes and the organization"* (Personal communication, 2024). In addition, another participant adds that "*EA plays an important role in assessing risks and threats to the business process and the organization as a whole"* (Personal communication, 2024), underscoring the need for a holistic approach to look at the enterprise in its environment.

Risk Identification

Participants agree that Risk Identification, which is the second step of the CRM process, will improve as well. One participant mentions: *"The integration of EA and security helps in identifying risks"* (Personal communication, 2024). Another participant adds that integrating CS and EA aids in the *"early identification of risks"* (Personal communication, 2024) Other participants have observed the same effects, with the most cautious statement being: "*I think it (the integration of EA and Cyber Security, red.) reasonably helps in identifying and mapping out what kind of risks are actually involved*" (Personal communication, 2024). A final participant remarked the role of Threat Modeling in identifying risks as early as possible in the process, because *"when you start developing something or if you have an existing architecture, you can already map out what potential risks exist in that architecture. I mean, we are doing far too little when it comes to what I would call Threat Modeling*" (Personal communication, 2024).

Risk Analysis and Risk Evaluation

The Risk Identification phase is followed by the Risk Analysis and Risk Evaluation phases. These phases are grouped together since there were only a few findings that could be mapped to these specific steps of the CRM process. A participant mentions that Risk Analysis and Evaluation will improve, by stating "*I think*

that if you have integrated it well, you are better able to shape Cyber Risk Management, actually assess your risks, and respond to them" (Personal communication, 2024). Another participant agrees, adding: *"EA plays an important role in assessing risks and threats to the business process and the organization as a whole"* (Personal communication, 2024). A final participant adds that the integration aids in "*Analyzing risks on application level*" (Personal communication, 2024), while similar benefits have been observed by other participants on the process level by another participant, arguing that with regards to Risk Identification and Risk Analysis: "*We need to focus more on the entire product and process, and Enterprise Architecture can really help to clarify the dependencies involved*" (Personal communication, 2024).

Risk Treatment

The most improvements were identified in the Risk Treatment phase. Integrating CS and EA leads to *"Better Risk Treatment"* (Personal communication, 2024). *"This allows you to map risks properly and reduce them to an acceptable level"* (Personal communication, 2024), adds another participant. The integration also leads to *"faster and more structural solutions for risk mitigation"* (Personal communication, 2024), *"aligning countermeasures better with the architecture"* (Personal communication, 2024), and *"incorporating mitigating measures into the architecture, resulting in a coherent approach to risk management"* (Personal communication, 2024).

Monitoring and Review

The final step in the CRM process is Monitoring and Review. According to one participant, integrating CS and EA helps with *"Validating whether measures have the desired effect on the product and the organization's resilience"* (Personal communication, 2024). Another participant adds that the integration of CS and EA helps with the *"measuring (the) effectiveness of security controls"* (Personal communication, 2024), because it is generally *"difficult to map the effectiveness of security measures"* (Personal communication, 2024). Therefore, integrating CS and EA could overcome the challenge of measuring the effectiveness of security measures on products and processes that the enterprise interacts with.

5 Discussion

This section analyzes the results and key findings of this research, comparing the empirical data with the literature presented in the Theoretical Background, see Chapter 2.

5.1 Interpretation of the Results

The results of my study highlighted several important themes related to enablers and blockers for integrating Cyber Security (CS) and Enterprise Architecture (EA). Among the challenges, participants noted that differences in mindset and focus between CS and EA teams, along with organizational misalignment and gaps in knowledge and skills, were significant blockers. These insights were consistent across both the Focus Group and interviews. One notable concern was the lack of sufficient knowledge on both sides: Enterprise Architects often lack in-depth security knowledge, while CS professionals have limited knowledge of EA. This knowledge gap hinders both teams from integrating, resulting in separate document creation and security being considered as an afterthought.

On the other hand, participants emphasized the importance of embedding security into EA frameworks and aligning CS and EA teams around a shared strategy and vision. In addition, the participants stressed the need for these teams to collaborate earlier in the process, making joint architectural decisions to ensure security is better integrated in architectural processes. The adoption of frameworks and development practices like DevSecOps and Secure by Design show that security is gradually being integrated into architectural processes, though these frameworks have not yet become standard practice across all organizations (Mees, 2016).

5.2 Comparison of the Literature

This section compares the main empirical findings to the literature in the Theoretical Background, see section 2.

1. **Embedding Cyber Security into EA Frameworks**

The first key finding from this research emphasizes the importance of embedding CS into EA frameworks, such as using SABSA. This integration allows for the establishment of normative sets of rules and guidelines that aid secure development in agile environments, ensuring that security is not merely an afterthought but a fundamental aspect of information system design. This finding is consistent with previous research on the intersection of CS and EA. For example, Diefenbach et al. (2019) found through their Literature Review that integrating security matters with EA viewpoints and frameworks is important, with current EA frameworks currently not able to meet that goal. In addition, Loft et al. (2021, p. 2) already documented challenges for integrating Security into EA frameworks, stating: "*Existing architecture*

frameworks typically require extensive knowledge of other standards and concepts." Furthermore, McClintock et al. (2020) identified several challenges in embedding security into EA frameworks, including a disjoint focus between teams and the absence of a thorough, research-driven approach in the development of these frameworks. Al-Turkistani et al. (2021) concluded, based on their review of EA frameworks, that none of the existing frameworks are fully suitable for integrating security aspects without significant modifications to the framework.

2. **Addressing knowledge gaps within both CS and EA teams regarding each other's domains**

Another key finding of this research is that a lack of sufficient knowledge and skills within both CS and EA teams regarding each other's domains was identified as a blocker for the integration of CS and EA**.** Prior research indicated that the absence of technical knowledge of non-security stakeholders was a common issue for the failure of (information) security programs (Loft et al., 2021). Larno et al., (2019, p. 60) identified a similar challenge, stating that (non-security) professionals involved in security policy development "*are provided with little knowledge about the processes they should follow. They often need to rely on guidelines which are not specifically designed for their organizations and thus fail to recognize and answer to their specific threats and requirements.*" No scientific publications were found that document insufficient EA knowledge of security professionals as a challenge, which can be explained because the literature on CS and EA integration is scant and most research focused on bringing security into EA, and not vice versa.

3. **Organizational misalignment, resulting in two distinct teams with different visions, strategies, and mindsets, working in isolation.**

My research has identified organizational misalignment as a challenge to integrating CS and EA, which is peculiar because EA is viewed as a holistic capability encompassing multiple domains, including business, technology, application, and data (Kotusev & Kurnia, 2021). Loft et al. (2021, p. 19) state: "*Effective security requires a holistic view of the whole company: its goals, processes, information flows, technology, people, and partners. EA provides this, by ensuring that technology is built on a sound architecture, where increasing complexity can be managed."* McClintock et al. (2020) along with a follow-up study by Graham et al. (2021), found that embedding a holistic security approach within EA improves communication between teams, strengthens security governance, and contributes to a more effective security program. This suggests that, despite EA's potential as a holistic framework for managing cyber risks, organizations continue to struggle with integrating CS and EA, often treating CS as a siloed function rather than an embedded part of the architectural approach.

This research also identified that the integration of CS and EA positively contributes to CRM within enterprises, with benefits identified in most of the CRM process steps (Eling et al., 2021). Participants observed that integrating CS and EA results in a better mapping of risks, allowing organizations to mitigate them effectively and reduce them to an acceptable level. This is in line with prior research on this topic. For

example, Nkambule et al. (2024) found that the relationships between different components of EA are critical in identifying dependencies and cyber risks, which in turn could be used for Risk Assessment. Loft et al. (2021) argue that EA can be used to determine important organizational assets and their true value by determining the sensitivity of data before conducting a Risk Assessment. The same logic was applied in the study of Diefenbach et al. (2019), where the authors stated the "*EA could provide input information for cyber risk Assessment*". This last statement was discussed in the Focus Group, where it was ranked fourth out of 6 (15.4%) on perceived importance by all participants, see Table 11. This highlights that while still important, other strategies were deemed more important by Focus Group participants.

5.3 Scientific Implications

This research makes several new contributions to the academic understanding of CS and EA integration, particularly in highlighting challenges and offering insights into organizational dynamics that affect this integration. One of the key findings relates to the ongoing difficulty of embedding CS into EA frameworks, despite the holistic capacity of EA to manage various organizational domains, including security. Unlike previous research that focused on the integration of CS and EA (e.g., Diefenbach et al., 2019; Graham et al., 2021; Loft et al., 2022; Mayer et al., 2019), this study provides empirical evidence showing that knowledge gaps, mindset differences, and organizational misalignment between CS and EA teams are significant barriers to the integration. These human and organizational factors have been underexplored in prior studies, offering a novel perspective on why these teams often struggle to work together effectively.

Additionally, this study contributes to the field by uncovering how better integration of CS and EA can enhance CRM, a topic that has not been extensively documented in existing literature. The research suggests that by integrating CS and EA, organizations can more effectively identify, assess, and mitigate cyber risks. This finding is particularly important because it shows that EA can play a crucial role in identifying risks earlier in the development process as well as streamlining risk treatment. The improved alignment between CS and EA facilitates quicker, more structured solutions to managing risks, leading to more proactive and efficient CRM practices.

A final contribution of this study is the emerging role of **agile and secure development methodologies**, such as DevSecOps and Security by Design, in the integration of CS and EA. This research suggests that implementing methodologies like DevSecOps and Security by Design could facilitate a more proactive integration of security into architectural processes, moving away from the traditional reactive focus on risk mitigation. By embedding Security by Design in architectural processes, these approaches could help shift the perception that security is an afterthought, particularly among non-security professionals. However, this research showed that organizations continue to face challenges in fully adopting these modern approaches, meaning that future research is needed to understand and mitigate these challenges.

6 Conclusion

The aim of this thesis was to understand how Cyber Security (CS) and Enterprise Architecture (EA) can be integrated in relation to Cyber Risk Management (CRM) within enterprises, by documenting strategies that positively contribute to this integration. The following Research Question (RQ) was developed to guide this research:

How can Cyber Security and Enterprise Architecture be integrated in relation to Cyber Risk Management within enterprises?

The general proposition in this research is that integrating CS and EA will lead to improved CRM in enterprises. Based on this proposition, I conducted a Focus Group discussion and four interviews with experts in the field, allowing for different perspectives and views to emerge on this topic. The results indicate that CS and EA are currently only partially integrated, with several blockers hindering further integration. In contrast, multiple enablers were identified that could enhance this integration. To answer the RQ, the final list of strategies that have been established based on this study can be found in Table 16.

Table 16. *Final list of strategies that can improve the integration of CS and EA*

Strategy	Description
By embedding CS into EA Frameworks	Integrating security considerations, such as principles, viewpoints, and requirements as a fundamental part of EA frameworks ensures security is a primary concern in the architectural development process and not an afterthought.
By improving in-depth knowledge in CS and EA teams	Improving in-depth security knowledge at the EA level as well as architectural knowledge on the CS level is crucial for shared understanding, awareness, and knowledge exchange.
By aligning CS and EA functions in the Organizational Structure	Creating a shared vision, strategy, mindset, and focus between the CS and EA functions can enhance collaboration and joint decision making.
By leveraging agile and secure development methodologies	Leveraging agile and secure methodologies such as Security by Design and DevSecOps ensures enterprises can implement CS measures proactively and holistically.

By adopting these strategies, enterprises could improve CRM because CS and EA teams work as a team instead of isolated units. Additionally, this research indicated that *if* CS and EA are integrated, CRM will improve throughout all steps of the process, because enterprises can identify, assess, and treat cyber

risks more proactively and efficiently. These findings contribute to the originality of this research since this was, to the best of my knowledge, not documented before. Therefore, I consider the general proposition of this research to be true, meaning that integrating CS and EA will indeed lead to Improved CRM in enterprises, as my research data suggests. Of course, this statement needs further rigorous validation and empirical evidence.

6.1 Practical Implications

This study has several practical contributions, because the strategies derived from this research contain actionable results for enterprises to improve how CS and EA are currently integrated.

First, enterprises should strive to embed CS within their EA Frameworks more efficiently and cost-effectively. By integrating CS into their EA frameworks, enterprises ensure that security is not considered an afterthought, but a core element of their operations. Second, enterprises that are adopting agile methodologies will benefit from incorporating Security by Design into their development programs. This can be achieved through DevSecOps, which is already widely documented. Third, enterprises must improve in-depth security knowledge of their Enterprise Architects, which could be facilitated through learning and development programs. A question that enterprises could ask themselves is: "*Do I have sufficient, in-depth Cyber Security knowledge in my EA board?"* At the same time, security professionals must be equipped with a better understanding of EA strategies and processes. Finally, enterprises should reflect on how their CS and EA teams are currently organized, both strategically and operationally. Is there true collaboration, or are these teams working in isolation? Are documents and decisions made together or separately? Understanding and addressing organizational misalignment is crucial for managing cyber risks more effectively and efficiently, as this research indicated.

6.2 Limitations

Despite the valuable insights of this study, several limitations should be acknowledged to ensure a balanced understanding of the findings and their implications.

The first significant limitation is the relatively small sample size. The data was collected through one Focus Group discussion (n=6) and four interviews with experts, with one participant joining both, leaving a total of nine individual contributions. This small sample size reduces the diversity of perspectives and experiences represented in the data. As a result, the findings may not fully capture all strategies that enterprises face when integrating CS and EA. This limitation restricts the generalizability of the findings and underscores the need for further studies with larger and more diverse participant pools (Recker, 2021).

Second, this study took a broad scope, because no distinctions were made between sectors, company size and or geographical locations. The integration of CS and EA could vary across these contexts. Especially Small and Medium Enterprises (SMEs) are known to struggle with implementing EA, let alone integrating CS and EA. This broad scope limits the ability to give sector specific advice and recommendations, potentially reducing the applicability of results to certain enterprises. Future research could benefit from a more scoped approach, focusing on certain enterprise types, sectors, or geographies specifically and comparing the results to this study.

Third, the exclusive use of qualitative data is another limitation. This study could have benefited from quantitative data to strengthen the results and extend and/or validate the findings. The use of quantitative data to further enhance the findings is another recommendation for future research.

Finally, this study acknowledges the existence of various schools of thought within EA but does not investigate them individually, particularly from a CS or CRM perspective. In the same way, EA frameworks such as TOGAF and Zachman offer different approaches to architecture, which could potentially influence how CS can be embedded in these frameworks. Future research could explore how different EA schools of thought and frameworks align with CS perspectives.

6.3 Future Research

In addition to the previously mentioned suggestions for future research aimed at addressing the limitations of this study, several other areas are worth exploring:

First, a potential avenue for future research is to investigate how enterprises can effectively integrate Cyber Security (CS) into Enterprise Architecture (EA) frameworks. Given that this has emerged as a key finding of this study, a standardized approach could greatly benefit organizations in aligning CS with their EA frameworks. In addition, research could focus on identifying the specific skills that EA professionals need to develop to facilitate effective integration of CS with EA.

Another promising research area involves creating metrics or frameworks to evaluate the success of CS and EA integration in enterprises. This could include examining how these integrated practices contribute to reducing cyber risk.

By addressing these potential research directions, future studies can expand on the findings of this research and enhance understanding of the effective integration of CS and EA. As enterprises continue to evolve and confront increasingly complex cyber risks, research in this field is crucial for providing actionable insights that empower organizations to successfully tackle these challenges.

7 References

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. In *Cyber Security and Applications* (Vol. 2). KeAi Communications Co. https://doi.org/10.1016/j.csa.2023.100031

Alam, S. (2023). *Cybersecurity: Past, Present and Future* [Adana Alparslan Turkes Science and Technology University]. https://doi.org/10.48550/arXiv.2207.01227

Alcántara, M., & Melgar, A. (2016). Risk Management in Information Security: A Systematic Review. *Journal of Advances in Information Technology*, *7*(1), 1–7. https://doi.org/10.12720/jait.7.1.1-7

Althonayan, A., & Andronache, A. (2018). Shifting from information security towards a cybersecurity paradigm. *ACM International Conference Proceeding Series*, 68–79. https://doi.org/10.1145/3285957.3285971

Althonayan, A., & Andronache, A. (2019). Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management Alignment. *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. https://doi.org/10.1109/CyberSA.2019.8899445

Al-Turkistani, H. F., Aldobaian, S., & Latif, R. (2021). Enterprise Architecture Frameworks Assessment: Capabilities, Cyber Security and Resiliency Review. *2021 1st International Conference on Artificial Intelligence and Data Analytics, CAIDA 2021*, 79–84. https://doi.org/10.1109/CAIDA51941.2021.9425343

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. In *European Journal of Operational Research* (Vol. 253, Issue 1, pp. 1–13). Elsevier B.V. https://doi.org/10.1016/j.ejor.2015.12.023

Azmi, R., Tibben, W. J., & Than Win, K. (2018). Review of cybersecurity frameworks: context and shared concepts. *Journal of Cyber Policy*, *3*(2), 258–283. https://ro.uow.edu.au/eispapers1

Band, I., Solutions, C. H., Engelsman, W., Feltus, C., & Paredes, S. G. (2019). *How to Model Enterprise Risk Management and Security with the ArchiMate ® Language*. https://publications.opengroup.org/w172

Barateiro, J., Antunes, G., & Borbinha, J. (2012). Manage risks through the Enterprise Architecture. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3297–3306. https://doi.org/10.1109/HICSS.2012.419

Becks, M. B. (2024). *Implementation of Control Activities in Scaled Agile Environments at Financial Service Providers to Improve Risk Management*. University of Twente.

Bell, E., Bryman, A., & Harley, B. (2022). *Business Research Methods* (5th ed.). Oxford University Press.

Blakley, B., Mcdermott, E., & Geer, D. (2001, September). Information Security is Information Risk Management. *New Security Paradigms Workshop*. https://doi.org/10.1145/508185.508187

Bobbert, Y., & Mulder, H. (2013). Group Support Systems research in the field of Business Information Security; a practitioners view. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 589–598. https://doi.org/10.1109/HICSS.2013.244

Boeken, J. (2024). From compliance to security, responsibility beyond law. *Computer Law & Security Review*, *52*, 105926. https://doi.org/10.1016/j.clsr.2023.105926

Böhme, R., Laube, S., & Riek, M. (2019). A Fundamental Approach to Cyber Risk Analysis. *Casualty Actuarial Society*, *12*(2), 161–185.

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

Burger, B., Kanbach, D. K., Kraus, S., Breier, M., & Corvello, V. (2023). On the use of AI-based tools like ChatGPT to support management research. *European Journal of Innovation Management*, *26*(7), 233–241. https://doi.org/10.1108/EJIM-02-2023-0156

Burkett, J. S. (2012). Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®. *Information Security Journal*, *21*(1), 47–54. https://doi.org/10.1080/19393555.2011.629341

Cebula, J. J., Popeck, M. E., & Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks Version 2 CERT ® Division*. http://www.sei.cmu.edu

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Diefenbach, T., Lucke, C., & Lechner, U. (2019). Towards an integration of information security management, risk management and enterprise architecture management - A literature review. *Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom*, *2019-December*, 326–333. https://doi.org/10.1109/CloudCom.2019.00057

Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: from sensemaking to practice. *Computers & Security*, *132*, 1–17. https://doi.org/10.1016/j.cose.2023.103372

Efe, A. (2023). A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT. *Journal of Auditing and Assurance Services*, *2023*(2), 185–205. http://orcid.org/0000-

Eling, M., Elvedi, M., & Falco, G. (2023). The Economic Impact of Extreme Cyber Risk Scenarios. *North American Actuarial Journal*, *27*(3), 429–443. https://doi.org/10.1080/10920277.2022.2034507

Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93–125. https://doi.org/10.1111/rmir.12169

European Commission. (2022). *Cyber Resilience Act*. European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454

European Parliament. (2022). *NIS2 Directive*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.ENG&toc=OJ%3AL%3A2022%3A333%3ATOC

Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., Wang, S. S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G., & Lin, H. (2019). Cyber risk research impeded by disciplinary barriers. *Science*, *366*(6469), 1066–1069. https://doi.org/10.1126/science.aaz4795

Francis, G. (2019). Enterprise Risk Management (ERM): Key Risks, Responses and Applications. In *2019 Enterprise Risk Management Symposium*. https://www.soa.org/globalassets/assets/files/resources/essays-monographs/2019-erm-symposium/mono-2019-erm-francis.pdf#page=4.09

George, A. S. (2024). *When Trust Fails: Examining Systemic Risk in the Digital Economy from the 2024 CrowdStrike Outage*. https://doi.org/10.5281/zenodo.12828222

Giuca, O., Popescu, T. M., Popescu, A. M., Prostean, G., & Popescu, D. E. (2021). A survey of cybersecurity risk management frameworks. *Advances in Intelligent Systems and Computing*, *1221 AISC*, 240–272. https://doi.org/10.1007/978-3-030-51992-6_20

Graham, M., Falkner, K., Szabo, C., & Yarom, Y. (2021). Security Architecture Framework for Enterprises. *International Conference on Enterprise Information Systems*, 883–904. https://orcid.org/0000-0003-0309-4332

Hoogervorst, J. (2009). *Enterprise Governance and Enterprise Engineering*. Springer Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-92671-9

IBM. (2024). *Cost of a Data Breach Report 2024*. https://www.ibm.com/reports/data-breach

Innerhofer-Oberperfler, F., & Breu, R. (2006). Using an Enterprise Architecture for IT Risk Management. *Information Security for South Africa*. https://digifors.cs.up.ac.za/issa/2006/Proceedings/Full/115_Paper.pdf

International Organization for Standardization. (2018). *ISO 31000:2018: Risk Management — Guidelines*. https://www.iso.org/standard/65694.html

International Organization for Standardization. (2022a). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/27001

International Organization for Standardization. (2022b). *ISO/IEC 27005:2022: Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. https://www.iso.org/standard/80585.html

International Organization for Standardization. (2022c). *ISO/IEC/IEEE 42010:2022: Software, systems and enterprise — Architecture description*. https://www.iso.org/standard/74393.html

International Organization for Standardization. (2023). *ISO/IEC 27032:2023: Cybersecurity — Guidelines for Internet security*. https://www.iso.org/standard/76070.html

Jarjoui, S., & Murimi, R. (2021). A framework for enterprise cybersecurity risk management. In *Advances in Cybersecurity Management* (pp. 139–161). Springer International Publishing. https://doi.org/10.1007/978-3-030-71381-2_8

Jiang, Y., Jeusfeld, M. A., Mosaad, M., & Oo, N. (2024). Enterprise architecture modeling for cybersecurity analysis in critical infrastructures — A systematic literature review. In *International Journal of Critical Infrastructure Protection* (Vol. 46). Elsevier B.V. https://doi.org/10.1016/j.ijcip.2024.100700

Jonkers, H., Lankhorst, M. M., Ter Doest, H. W. L., Arbab, F., Bosma, H., & Wieringa, R. J. (2006). Enterprise architecture: Management tool and blueprint for the organisation. *Information Systems Frontiers*, *8*(2), 63–66. https://doi.org/10.1007/s10796-006-7970-2

Klein, E. E., Tellefsen, T., & Herskovitz, P. J. (2007). The use of group support systems in focus groups: Information technology meets qualitative research. *Computers in Human Behavior*, *23*(5), 2113–2132. https://doi.org/10.1016/j.chb.2006.02.007

Kordy, B., Mauw, S., Radomirovic, S., & Schweitzer, P. (2014). Attack-defense trees. *Journal of Logic and Computation*, *24*(1), 55–87. https://doi.org/10.1093/logcom/exs029

Korhonen, J. J., Lapalme, J., McDavid, D., & Gill, A. Q. (2016). Adaptive Enterprise Architecture for the Future: Towards a Reconceptualization of EA. *Proceedings - CBI 2016: 18th IEEE Conference on Business Informatics*, *1*, 272–281. https://doi.org/10.1109/CBI.2016.38

Kotusev, S. (2016a). *Enterprise Architecture Is Not TOGAF*. British Computer Science. https://kotusev.com/Enterprise%20Architecture%20Is%20Not%20TOGAF.pdf

Kotusev, S. (2016b). The History of Enterprise Architecture: An Evidence-Based Review. In *Journal of Enterprise Architecture* (Vol. 12, Issue 1).

Kotusev, S. (2018). Enterprise Architecture: A Reconceptualization Is Needed. *Pacific Asia Journal of the Association for Information Systems*, 1–36. https://doi.org/10.17705/1pais.10401

Kotusev, S. (2019). Enterprise architecture and enterprise architecture artifacts: Questioning the old concept in light of new findings. *Journal of Information Technology*, *34*(2), 102–128. https://doi.org/10.1177/0268396218816273

Kotusev, S. (2020). *What Is Agile Enterprise Architecture?* http://kotusev.com

Kotusev, S., & Kurnia, S. (2021). The theoretical basis of enterprise architecture: A critical review and taxonomy of relevant theories. *Journal of Information Technology*, *36*(3), 275–315. https://doi.org/10.1177/0268396220977873

Kotusev, S., Kurnia, S., & Dilnutt, R. (2022). The practical roles of enterprise architecture artifacts: A classification and relationship. *Information and Software Technology*, *147*. https://doi.org/10.1016/j.infsof.2022.106897

Kotusev, S., Kurnia, S., Dilnutt, R., & van de Wetering, R. (2024). The Structuring of Enterprise Architecture Functions in Organizations: Towards a Systematic Theory. *Business and Information Systems Engineering*, *66*(4), 465–488. https://doi.org/10.1007/s12599-023-00845-4

Kotusev, S., Singh, M., & Storey, I. (2017). A Frameworks-Free Look at Enterprise Architecture. In *Journal of Enterprise Architecture* (Vol. 13, Issue 1).

Kurnia, S., Kotusev, S., Dilnutt, R., Taylor, P., Shanks, G., & Milton, S. (2020). Artifacts, Activities, Benefits and Blockers: Exploring Enterprise Architecture Practice in Depth. *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 5583–5592. https://hdl.handle.net/10125/64429 978-0-9981331-3-3

Lankhorst, M. (2017). *Enterprise Architecture at Work Modelling, Communication and Analysis* (4th ed.). Springer Berlin, Heidelberg. https://doi.org/https://doi.org/10.1007/978-3-662-53933-0

Lapalme, J. (2012). Three Schools of Thought on Enterprise Architecture. *IT Professional*, *14*(6), 37–43. https://doi.org/10.1109/MITP.2011.109

Larno, S., Seppänen, V., & Nurmi, J. (2019). Method Framework for Developing Enterprise Architecture Security Principles. *Complex Systems Informatics and Modeling Quarterly*, *2019*(20), 57–71. https://doi.org/10.7250/csimq.2019-20.03

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Loft, P., He, Y., Janicke, H., & Wagner, I. (2021). Dying of a hundred good symptoms: why good security can still fail - a literature review and analysis. *Enterprise Information Systems*, *15*(4), 448–473. https://doi.org/10.1080/17517575.2019.1605000

Loft, P., He, Y., Yevseyeva, I., & Wagner, I. (2022). CAESAR8: An agile enterprise architecture approach to managing information security risks. *Computers and Security*, *122*. https://doi.org/10.1016/j.cose.2022.102877

Macnish, K., & Van der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in Society*, *63*. https://doi.org/10.1016/j.techsoc.2020.101382

Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E., & Wieringa, R. (2019). An integrated conceptual model for information system security risk management supported by enterprise architecture management. *Software and Systems Modeling*, *18*(3), 2285–2312. https://doi.org/10.1007/s10270-018-0661-x

Mayer, N., Grandry, E., Feltus, C., & Goettelmann, E. (2015). Towards the entri framework: Security risk management enhanced by the use of enterprise architectures. *Lecture Notes in Business Information Processing*, *215*, 459–469. https://doi.org/10.1007/978-3-319-19243-7_42

McClintock, M., Falkner, K., Szabo, C., & Yarom, Y. (2020). Enterprise security architecture: Mythology or methodology? *ICEIS 2020 - Proceedings of the 22nd International Conference on Enterprise Information Systems*, *2*, 679–689. https://doi.org/10.5220/0009404406790689

Mees, W. (2016). *Security by Design in an Enterprise Architecture Framework*. NATO Science & Technology Organization. https://doi.org/10.14339/STO-EN-IST-143-06-PDF

Molnar, W. A., & Proper, H. A. (2013). Engineering an enterprise: Practical issues of two case studies from the Luxembourgish beverage and tobacco industry. In F. Harmsen & Henderik. A. Proper (Eds.), *Working Conference on Practice-Driven Research on Enterprise Transformation* (pp. 76–91).

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

Niemi, E. (2006). Enterprise Architecture Benefits: Perceptions from Literature and Practice. In K. Soliman (Ed.), *Proceedings of the 7th international business information management association (IBIMA) conference on internet and information systems in the digital age*. IBIMA Publishing.

Niemi, E., & Pekkola, S. (2020). The Benefits of Enterprise Architecture in Organizational Transformation. *Business and Information Systems Engineering*, *62*(6), 585–597. https://doi.org/10.1007/s12599-019-00605-3

Nkambule, M., Jansen Van Vuuren, J., & Leenen, L. (2024). Integrating Enterprise Architecture into Cybersecurity Risk Management in Higher Education. *International Conference on Cyber Warfare and Security 19(1)*, 501–510. https://doi.org/https://doi.org/10.34190/iccws.19.1.2189

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, *16*(1). https://doi.org/10.1177/1609406917733847

Oda, M., Fu, H., & Zhu, Y. (2009). *Enterprise information security architecture: A review of frameworks, methodology, and case studies*. IEEE. https://doi.org/10.1109/iccsit.2009.5234695

Oliveira, Í., Prince Sales, T., Paulo Almeida, J. A., Baratella, R., Fumagalli, M., & Guizzardi, G. (2022). Ontological Analysis and Redesign of Security Modeling in ArchiMate. In B. S. Barn & K. Sandkuhl (Eds.), *The Practice of Enterprise Modeling* (pp. 82–98). Springer. https://doi.org/https://doi.org/10.1007/978-3-031-21488-2_6

Plessius, H., Steenbergen, M. van, Slot, R., & Versendaal, J. (2018). The Enterprise Architecture Value Framework. *Research-in-Progress Papers*, 11–29. https://aisel.aisnet.org/ecis2018_rip/48

Pöhn, D., Seeber, S., & Hommel, W. (2023). Combining SABSA and Vis4Sec to the Process Framework IdMSecMan to Continuously Improve Identity Management Security in Heterogeneous ICT Infrastructures. *Applied Sciences (Switzerland)*, *13*(4). https://doi.org/10.3390/app13042349

PRISM. (1986). *Dispersion and Interconnection: Approaches to Distributed Systems Architecture*. https://cdn.ymaws.com/www.globalaea.org/resource/collection/EAAC3D6C-D447-451C-AC5F-6E1DC7788D42/PRISM_Report.pdf

Proper, H. A., & Lankhorst, M. M. (2014). Enterprise Architecture Towards essential sensemaking. *Enterprise Modelling and Information Systems Architectures*, *9*(1), 5–21. https://doi.org/10.18417/emisa.9.1.1

Pulkkinen, M., Naumenko, A., & Luostarinen, K. (2007). Managing information security in a business network of machinery maintenance services business - Enterprise architecture as a coordination tool. *Journal of Systems and Software*, *80*(10), 1607–1620. https://doi.org/10.1016/j.jss.2007.01.044

Recker, J. (2021). *Scientific Research in Information Systems* (2nd ed.). Springer Cham. http://www.springer.com/series/10440

Refsdal, A., Solhaug, B., & Stolen, K. (2015). *Cyber-Risk Management*. Springer Cham. https://doi.org/10.1007/978-3-319-23570-7

Roberts, L. (1986). THE ARPANET AND COMPUTER NETWORKS. *The History of Personal Workstations*, 51–58. https://doi.org/https://doi.org/10.1145/12178.12182

Ross, J. W., Weill, P. D., & Robertson, D. C. (2006). *Enterprise Architecture as Strategy — Creating a Foundation for Business Execution*. Harvard Business School Press.

Ruan, K. (2019). Cyber Risk Management: A New Era of Enterprise Risk Management. In *Digital Asset Valuation and Cyber Risk Management* (pp. 49–73). Elsevier. https://doi.org/10.1016/b978-0-12-812158-0.00003-x

Ruthberg, Z. G., & McKenzie, R. G. (1977, March). *Audit and evaluation of computer security*. https://doi.org/10.6028/NBS.SP.500-19

Saint-Louis, P., & Lapalme, J. (2018). An exploration of the many ways to approach the discipline of enterprise architecture. In *International Journal of Engineering Business Management* (Vol. 10). SAGE Publications Inc. https://doi.org/10.1177/1847979018807383

Saint-Louis, P., Morency, M. C., & Lapalme, J. (2019). Examination of explicit definitions of enterprise architecture. In *International Journal of Engineering Business Management* (Vol. 11). SAGE Publications Inc. https://doi.org/10.1177/1847979019866337

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining Confidentiality, Integrity, and Availability in Security. *Journal of Information System Security*, *10*(3), 21–45. www.jissec.org

Scholtz, T. (2006). *Structure and Content of an Enterprise Information Security Architecture*. Gartner, Inc. https://www.gartner.com/en/documents/488195

Shankar, K. S. (1977). The Total Computer Security Problem: An Oveview. *Computer*, *10*(6), 50–73. https://doi.org/10.1109/c-m.1977.217748

Sherwood, J., Clark, A., & Lynas, D. (2005). *Enterprise Security Architecture*. CRC Press.

Shopovski, J. (2024). *Generative Artificial Intelligence, AI for Scientific Writing: A Literature Review*. https://doi.org/10.20944/preprints202406.0011.v1

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Steenbergen, M. van. (2023). The Need for New Architectural Truths. In *Digital Enterprises* (pp. 201–210). Springer Cham. https://doi.org/10.1007/978-3-031-30214-5_15

Stine, K., Quinn, S., Witte, G., & Gardner, R. K. (2020). *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. https://doi.org/10.6028/NIST.IR.8286

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *135*. https://doi.org/10.1016/j.ssci.2020.105143

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. *IEEE Communications Surveys and Tutorials*, *VOL. 25, NO. 3*(THIRD QUARTER 2023). https://doi.org/10.1109/COMST.2023.3273282

The Open Group. (2022a). *Integrating Risk and Security within a TOGAF® Enterprise Architecture*. https://pubs.opengroup.org/togaf-standard/integrating-risk-and-security/

The Open Group. (2022b). *Open Agile Architecture*. https://pubs.opengroup.org/architecture/o-aa-standard-single/

The Open Group. (2022c). *The TOGAF® Standard, 10th Edition*. https://pubs.opengroup.org/togaf-standard/

Vallerand, J., Lapalme, J., & Moïse, A. (2017). Analysing enterprise architecture maturity models: a learning perspective. *Enterprise Information Systems*, *11*(6), 859–883. https://doi.org/10.1080/17517575.2015.1091951

Van Wessel, R. M., Kroon, P., & De Vries, H. J. (2023). Scaling Agile Company Wide: The Organizational Challenge of Combining Agile Scaling Frameworks and Enterprise Architecture in Service Companies. *IEEE Engineering Management Review*, *51*(3), 25–32. https://doi.org/10.1109/EMR.2023.3277128

Villalón-Fonseca, R. (2022). The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity. *Computers and Security*, *120*. https://doi.org/10.1016/j.cose.2022.102805

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

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

Ware, W. H. (1970). *Security Controls for Computer Systems*. https://conferences.computer.org/sp/pdfs/early/ware70.pdf

World Economic Forum. (2024). *The Global Risks Report 2024*. www.weforum.org

Zachman, J. A. (1987). A framework for information systems architecture. *IBM Systems Journal*, *38*(2.3), 454–470. https://doi.org/10.1147/sj.382.0454

Zhang, H., Han, W., Lai, X., Lin, D., Ma, J., & Li, J. (2015). Survey on cyberspace security. *Science China Information Sciences*, *58*(11), 1–43. https://doi.org/10.1007/s11432-015-5433-4

Appendices

Appendix A: Overview of Core Publications

Table A1 describes the core publications used in this research. These are the publications that can be retrieved by executing one of the search queries in section 3.3.1.

Table 17. *Core Publications*

No.	Authors	Year	Title	Conference/Journal	Peer Reviewed?
1	McClintock et al.	2020	Enterprise security architecture: Mythology or methodology?	International Conference on Enterprise Information Systems	Yes
2	Loft et al.	2019	Dying of a Hundred Good Symptoms: Why Good Security Can Still Fail - A Literature Review and Analysis of Enterprise Information Security Architectures (EISAs)	Enterprise Information Systems, Vol. 15	Yes
3	Loft et al.	2022	CAESAR 8: An agile enterprise architecture approach to managing information security risks	Computers and Security (2022) 122	Yes
4	Diefenbach et al.	2019	Towards an Integration of Information Security Management, Risk Management and Enterprise Architecture Management – A Literature Review	IEEE International Conference on Cloud Computing Technology and Science 2019	Yes
5	Al-Turkistani et al.	2023	Enterprise Architecture Frameworks Assessment: Capabilities, Cyber Security and Resiliency Review	1st International Conference on Artificial Intelligence and Data Analytics (CAIDA)	Yes
6	Shariati et al.	2011	Enterprise information security, a review of architectures and frameworks from interoperability perspective	Procedia Computer Science 3 (2011) 537–543	Yes

7	Jiang et al.,	2024	Enterprise architecture modeling for cybersecurity analysis in critical infrastructures — A systematic literature review	International Journal of Critical Infrastructure Protection	Yes
8	Ekstedt & Sommestad	2009	Enterprise Architecture Models for Cyber Security Analysis	IEEE PES Power Systems Conference and Exposition	Yes
9	Mayer et al.	2019	An integrated conceptual model for information system security risk management supported by enterprise architecture management	Software & Systems Modeling	Yes
10	Innerhofer-Oberperfler & Breu	2006	Using an enterprise Architecture for IT Risk Management	Information Security for South Africa	Yes
11	Grandry et al.	2013	Conceptual Integration of Enterprise Architecture Management and Security Risk Management	17th IEEE International Enterprise Distributed Object Computing Conference Workshops	Yes
12	Larno et al.	2012	Method Framework for Developing Enterprise Architecture Security Principles	Complex Systems Informatics and Modeling Quarterly	Yes

Appendix B: Focus Group Protocol

Introductie en inloop (10 minuten)

Vanuit het lectoraat Cyber Security en de Master of Informatics (MOI) van de Hogeschool Utrecht voer ik een onderzoek uit naar de integratie tussen Enterprise Architecture (EA) en Cyber Security ten behoeve van Cyber Risk Management in organisaties. Het doel van het onderzoek is om inzicht te verkrijgen in bestaande ervaringen en perspectieven met betrekking tot deze integratie, en het effect ervan op Cyber Risk Management. We streven naar een beter begrip van de uitdagingen en kansen op dit gebied.

Gedurende deze Focus Group maken we gebruik van Meetingwizard om antwoorden op te halen en de discussie over dit onderwerp te faciliteren. De antwoorden die hier worden gegeven zullen geanonimiseerd verwerkt worden in het onderzoek, mits daar goedkeuring is voor gegeven door middel van het retour sturen van het informed consentformulier.

Naar Meeting Wizard -

Open vragen (25 minuten)

In hoeverre zijn Enterprise Architectuur en Cyber Security geïntegreerd binnen organisaties vanuit jouw ervaring?

[Antwoordscore van 1 tot 5, waarbij 1 laag is en 5 hoog]

Hoe komt het dat nog niet 'beter geïntegreerd is?

Hoe komt het dat het al 'zo goed' is geïntegreerd?

Wat is de impact van deze integratie op cyber risico's?

Verdiepende vraag: Wat zijn blockers voor de integratie van EA en Cyber Security?

Hoe speelt Enterprise Architecture een rol bij het bepalen van de impact van cyber risico's op de bedrijfsdoelstellingen?

Lijst met factoren

Uit de literatuur (score van 100 toekennen/verdelen)

Welke practices/ervaringen kunnen jullie vanuit jullie ervaring toevoegen aan deze lijst?

Kunt u specifieke voorbeelden delen van hoe uw organisatie Enterprise Architecture en Cyber Security succesvol heeft geïntegreerd om effectief om te gaan met cyber risico's?

Welke methoden of benaderingen hanteert uw organisatie om de samenwerking tussen Cyber Security- en Enterprise Architecture-teams te faciliteren bij het identificeren en aanpakken van beveiligingsrisico's? (Optioneel)

Kunt u voorbeelden delen van succesvolle integraties tussen Enterprise Architecture en Cyber Security die hebben bijgedragen aan een effectievere cyberrisicomanagementstrategie?

Wat is de impact op de mate van integratie tussen EA en Cyber Security in relatie tot managen van cyberrisico's?

Validatieronde (10 min)

Geef aan bij elk van onderstaande 'practices' (praktijken) aan hoe waardevol deze zijn voor de integratie van EA en Cybersecurity ten behoeve van Cyber Risk Management:

[Antwoordscore van 1 tot 5, waarbij 1 laag is en 5 hoog]

- De integratie van business requirements met security requirements
- Het toepassen van 'security-by-design' zodat security wordt meegenomen vanaf het begin van de levenscyclus van een EA-asset
- De integratie van security viewpoints in EA frameworks (bijv. TOGAF)
- Het integreren van Cyber Security in EA modeling (bijv. via UML of ArchiMate)
- Het integreren van Business & IT activiteiten (Business & IT alignment) zodat de organisatie inspanningen om cyberrisico's te bestrijden beter kan coördineren

Open discussie (20 min)

Zijn er nog andere voorbeelden die niet eerder benoemd zijn die relevant zijn voor de integratie van EA en Cyber Security ten behoeve van Cyber Risk Management?

Zijn er nog andere vragen en/of opmerkingen met betrekking tot dit onderzoek?

Afsluiting (5 min)

Bedanken voor de tijd

Toelichting wat er met de antwoorden wordt gedaan

Appendix C: Interview Protocol

Introductie

- Bedank voor tijd en deelname aan het onderzoek
- Korte toelichting onderzoek
- Toestemmingsverklaring
- Zijn er vooraf vragen?
- Vraag of de opname gestart mag worden en licht toe waar de opname voor wordt gebruikt

Open vragen

1. In hoeverre zijn Enterprise Architectuur en Cyber Security geïntegreerd binnen organisaties vanuit jouw ervaring?
2. Wat zijn blockers voor de integratie van EA en Cyber Security in organisaties?
3. Wat zijn enablers voor de integratie van EA en Cyber Security in organisaties?
4. Wat is de impact van de integratie tussen EA en Cyber Security op cyberrisicomanagement?
    - Waaruit blijkt dat de integratie beter/slechter wordt?
5. Zijn er specifieke onderdelen van cyberrisicomanagement die beter/slechter worden?
    - Denk aan: risk identification, analysis, evaluation, treatment

Validatie factoren

Toon factoren uit de literatuur en de Focus Group op het scherm (via Teams/PowerPoint)

1. Kan je aangeven welke van deze factoren je het meest relevant vindt voor de integratie van EA en Cyber Security?
    - En waarom is dat relevant voor jou / kan je voorbeelden noemen?
2. Welke van de factoren vind je het minst relevant voor de integratie van EA en Cyber Security?
3. Zijn er vanuit jouw ervaring nog factoren die missen in deze lijst?
    - Kan je toelichten waarom je die factoren mist / kan je voorbeelden noemen?

Afsluiting

1. Zijn er nog zaken die je wil toevoegen?
2. Heb je vragen en/of opmerkingen over het interview?
    - Stop recording.
    - Dank nogmaals voor deelname aan het onderzoek en de tijd

EINDE

Appendix D: Informed Consent Form

Voor deelname aan het onderzoek: **Integratie van EA en cyber Security ten behoeve van Cyber Risk Management**

Toelichting onderzoek: Vanuit het lectoraat Cyber Security en de Master of Informatics (MOI) van de Hogeschool Utrecht voer ik een onderzoek uit naar de integratie tussen Enterprise Architecture en Cyber Security in relatie tot Cyber Risk Management in organisaties. Het doel van het onderzoek is om inzicht te verkrijgen in bestaande ervaringen en perspectieven met betrekking tot deze integratie, en het effect ervan op Cyber Risk Management. We streven naar een beter begrip van de uitdagingen en kansen op dit gebied.

U heeft aangegeven mee te willen doen aan de Focus Groep, het interview of beide. Hartelijk dank daarvoor. Middels dit formulier vraag ik toestemming voor het verwerken van Focus Group en/of interviewdata en informeer ik wat uw rechten zijn bij deelname aan dit onderzoek.

Voor verdere vragen kunt u contact opnemen met Nick Nieuwenhuis via nick.nieuwenhuis@student.hu.nl.

Inleiding toestemmingsverklaring:

1. Ben ik over aard, methode en doel van dit onderzoek op een voor mij duidelijke wijze geïnformeerd;
2. Heb ik genoeg tijd gekregen om over deelname te beslissen;
3. Heb ik de gelegenheid gehad om vragen te stellen over dit onderzoek;
4. Weet ik dat deelname vrijwillig is;
5. Weet ik dat ik op elk gewenst moment kan stoppen met deelnemen aan het onderzoek. Daarvoor hoef ik geen reden te geven;
6. Geef ik toestemming voor het verzamelen, bewaren en gebruiken van mijn gegevens voor de beantwoording van de onderzoeksvraag in dit onderzoek;
7. Weet ik dat de uitkomsten van dit interview verwerkt kunnen worden in een verslag of (wetenschappelijke dan wel praktijkgerichte) publicaties;
8. Begrijp ik dat alle informatie die ik met betrekking tot deze studie verstrek, zal worden gepseudonimiseerd, waardoor het niet direct naar mij herleidbaar zal zijn;
9. Weet ik dat ik inzage kan krijgen in de wijze waarop de gegevens worden verwerkt en bewaard;
10. Weet ik dat als ik mij terugtrek, mijn gegevens tot dat moment gebruikt kunnen worden, tenzij ik ook vraag om de reeds verzamelde gegevens te wissen;
11. Geef ik toestemming tot het maken van een audio-opname van de Focus Group en/of het interview. Deze opname wordt op beveiligde wijze, geautomatiseerd omgezet in een transcript en is verder alleen te beluisteren door de onderzoekers en ter controle van de wetenschappelijke integriteit van de onderzoekers en de onderzoeksproducten.

Invullen deelnemer:

1. **Bij deze geef ik akkoord op eerdergenoemde stellingen**

- Akkoord
- Niet akkoord

2. **Wat is uw naam? (Deze wordt gepseudonimeerd)**

3. **Wat is uw functie** (deze wordt gebruikt om de integriteit/kwaliteit van de beantwoording van de onderzoeksvraag te motiveren)

4. **Ik wil graag op de hoogte worden gehouden van de resultaten van het onderzoek**

- Ja
- Nee

5. **Wilt u nog iets toevoegen?**

Appendix E: Blockers – Codes and Themes

Table 18. *Full List of Blockers, Organized per Theme*

Themes	Codes / Blockers
Lack of Awareness and Reactive Security Approach	- Security is reactive - Security is forgotten by EA - Security is operationally driven - Security is an after-thought - Security comes in late in the process
Skills & Knowledge Gaps	- Lack of knowledge at the EA level - Enterprise Architect has no in-depth security knowledge - Lack of threat modelling - Knowledge gaps
Process and Strategic Misalignment	- Lack of alignment between EA and cyber security - No overarching strategy - Own communication channels - Cultural differences in problem-solving - Different perspectives - Different focus - Different mindsets - Separate worlds - Thinking in silos
Technical Misalignment	- IT is seen as a different field from architecture - Cyber security requirements not included in EA - EA thinks functionally, risks insufficiently covered - Information processing not considered at EA level - Security developments not incorporated - Outdated architecture diagrams
Organizational Structure	- Organizationally disconnected - Lack of hierarchical lines - Different reporting lines - Lack of hierarchical guidance - Struggles with cooperation in the hierarchy - Different functions within the organization - Different reporting lines - No relationship established between EA and Security

Appendix F: Enablers – Codes and Themes

Table 19. *Full list of Enablers, Organized per Theme*

Themes	Enablers
Leadership and Strategic Alignment	- Commitment from higher management - Senior management is engaged in EA and Cybersecurity integration - The same manager should oversee EA and Cybersecurity (ideal) - EA architects and CISO should follow the same strategy - Having a shared strategy
Collaboration and Shared Responsibility	- Creating a shared vision - Cyber, architecture, and business are at the same table - Speak each other's language - Joint document creation - Partnership between EA and security - Security responsibility lies with autonomous DevOps teams - The responsible person for products or services is accountable for security - Collaboration between EA and CISO - Shared platforms
Security Integration into EA Frameworks	- Better integration of security and business requirements in EA - Security modelled in EA - Security embedded in EA frameworks - Security features included earlier in development processes - Security integrated into architecture - Security is a capability in EA - Security principles in architecture principles - Security requirements considered in product and vendor selection
Security Awareness and Organizational Culture	- Security awareness at EA level - Awareness about security - Knowledge of processes and the organization - More awareness of cybersecurity - Understanding the human factor - Making measures and integration more measurable - Policies must align with practice

Holistic and Standardized Approaches	- Holistic approach to security is important - Looking at the whole ecosystem to map the end-to-end process - Standardization in architecture - Security integrated at process level instead of application level - Splitting responsibilities - Business decisions better reflected in security decisions

Appendix G: Cyber Risk Management – Codes and Themes

Table G1. *Mapping of Codes to the Cyber Risk Management Process*

Cyber Risk Management process steps	Codes
Context Establishment	- EA plays a key role in assessing risks and threats to the business process and the organization as a whole - Knowledge of processes and the organization
Risk Identification	- The integration of EA and security helps in identifying risks - Risks covered earlier - Threat modelling helps to identify risk scenarios, verify, and mitigate - Identifying risks early - Identify risk early and mitigate to an acceptable level
Risk Analysis & Evaluation	- Risk analysis on applications - Improved Risk Assessment - Understand role of third parties
Risk Treatment	- Countermeasures better align with the architecture - Mitigating measures are integrated into the architecture, improving response to risks - More variations in measures, creating options - Faster and structural solutions for risk mitigation - Better risk treatment - Integration leads to a shred interest in mitigating risks
Monitoring & Review	- Validate whether the measures have the desired effect on the product and the resilience of the organization - Measures should be measurable - Validating whether the measures have the desired effect
Miscellaneous	- Standardization in Risk Management - More efficient Risk Management - Improved Cyber Risk Management - Cyber Risk Management becomes better, more reliable and more predictable

Towards the Integration of Cyber Security and Enterprise Architecture to Improve Cyber Risk Management

Nick Nieuwenhuis

https://doi.org/10.5281/zenodo.14639415