Master Degree Project

Clarifying Roles and Responsibilities in Information Security

A Case Study of Policy Implementation in High-Stakes Environments

Tara Alndawi

Supervisor: Martin Lundgren
Examiner: Marcus Nohlberg

Master Degree Project (120 ECTS) in Informatics with a Specialization in Privacy, Information and Cyber Security
Advanced level 30 ECTS
Spring term 2024

Abstract

In information security, the success of security policies is critically dependent on their implementation in organizations. This thesis explores the gap between formal definitions and the actual implementation of security policies, focusing on roles within a Swedish defense company. Using a qualitative research approach, this study employs semi-structured interviews to gather in-depth insights from individuals directly involved in security management, with the aim of uncovering the real-world complexities and challenges faced in policy implementation. This study identifies several core issues that affect policy implementation: ambiguity in role definitions, inconsistencies in policy communication at different organizational levels, and the frequent need for individuals to adapt policies to practical and situational needs. These factors contribute to the risk of security breaches by creating conditions in which policies are misunderstood or incorrectly applied. The findings highlight a significant discrepancy between how policies are intended to function and how they are implemented in daily operations, revealing a critical vulnerability in organizational security frameworks. This thesis contributes to the existing body of knowledge by mapping the landscape of security policy implementation within the context of the highly regulated defense industry. The results provide empirical evidence that improves the understanding of the interaction between policy, practice and the human element in security regimes with the aim of improving clarity and reducing the incidence of human error in security practices.

Keywords: practical policy application, policy compliance, security policy gaps , role clarity, role ambiguity, information security management, Swedish defense industry

Acknowledgement

In loving memory of my Jiddu, Beden Fadhel Alnidawi, I pledge to lead with intellect and courage, standing firm for my beliefs and rights, just as you did. Every achievement is a tribute to your bravery and sacrifice.

To my parent, your sacrifices have not gone unnoticed, and I am forever grateful for the love and stability you have provided me. This achievement is not just my own, but a testament to your enduring love and commitment. Thank you, Mom and Dad, for everything you have done and continue to do.

To my husband, thank you for being my rock during these intense years of study. Your unwavering support and love have been the light that guided me through late nights and challenging moments. You believed in me on the days I doubted myself and celebrated every small victory along the way. I will forever be grateful for your love, strength, and kindness.

Martin Lundgren, having you as my supervisor has been invaluable. Thank you for your patience and wisdom, for consistently encouraging me to engage in more in-depth thought, and for your unwavering support during this academic journey.

Contents

1 Introduction **1**
- 1.1 Problem Definition . . . 2
- 1.2 Aim and Objectives . . . 2
- 1.3 Research Structure . . . 2

2 Background **4**
- 2.1 Preliminaries . . . 4
  - 2.1.1 Information Security . . . 4
  - 2.1.2 The Human Element . . . 5
  - 2.1.3 Information Security Management . . . 6
  - 2.1.4 Roles and Responsibilities . . . 7
- 2.2 Research background . . . 8
  - 2.2.1 Standardized Policies to Practical Implementation . . . 8
  - 2.2.2 Practical Challenges in Security Policy Integration . . . 10
- 2.3 Contribution . . . 11

3 Method **12**
- 3.1 Research Design . . . 12
  - 3.1.1 Selection of Case Company . . . 12
- 3.2 Data Collection . . . 13
- 3.3 Data Analysis . . . 15
  - 3.3.1 Thematic Analysis . . . 15
- 3.4 Reliability and Validity . . . 17
- 3.5 Delimitation . . . 17
- 3.6 Ethical Considerations . . . 18

4 Result **20**
- 4.1 Thematic Coding . . . 20
- 4.2 Findings . . . 21
  - 4.2.1 Formal Roles and Practical Realities . . . 21
  - 4.2.2 Challenges in Role Clarity and Responsibilities . . . 21
  - 4.2.3 Communication of Roles and Responsibilities . . . 23
  - 4.2.4 Role Flexibility and Individual Adaption . . . 23
  - 4.2.5 Enhancing Role Clarity . . . 24

5 Analysis of Result **25**
- 5.1 Formal Roles and Practical Realities . . . 25
- 5.2 Challenges in Role Clarity and Responsibilities . . . 26
- 5.3 Communication of Roles and Responsibilities . . . 26
- 5.4 Role Flexibility and Individual Adaption . . . 26
- 5.5 Enhancing Role Clarity . . . 26

6 Discussion **27**
- 6.1 Theoretical Framework . . . 27
  - 6.1.1 Relation to Previous Research . . . 27
  - 6.1.2 New Insights to Previous Research . . . 28
- 6.2 Methods, Implementation and Results . . . 28

6.3 Ethical and societal aspects 29

7 Conclusion **31**
7.1 Future work 32

A Interview Guide in Swedish **I**

B Appendix: Interview Guide in English **III**

1 | Introduction

Despite advances in technical safeguards for information systems, human error continues to play a significant role in the escalation of cybersecurity breaches (Amorosa and Yankson, 2023). A survey conducted by PwC in 2015 revealed that 50% of the worst breaches experienced by organizations were due to unintentional human error (PwC, 2015). A large percentage of organizations reported suffering from employee related security breaches. For large organizations, this number was 75%, and 31% for small businesses. The data from the PwC survey illustrate that a substantial portion of organizations experience breaches directly related to employee errors, especially among large organizations. A recent study by Hancock and Tessian (2022) shows that 88% of data breaches were due to simple human errors. This statistic is supported by World Economic Forum (2022), which attributes 95% of all cybersecurity issues to human error highlighting the severe financial consequences, with the global average cost of a data breach in 2023 reaching $4.45 million, a 15% increase over the past three years (IBM, 2023). Such statistics highlight the pressing need for clear policies that define roles and responsibilities to effectively mitigate human errors. The importance of addressing human vulnerabilities in safeguarding information systems is highlighted by Stewart and Jürjens (2017), who emphasize the need to comply with security policies and robust training to mitigate risks associated with employee actions. Similarly, Costantino et al. (2018) point out how social engineering exploits human weaknesses, arguing that technical defenses, while necessary, are not sufficient on their own. Attackers recognize that humans are prone to errors, may overlook details or do not fully understand the consequences of their actions, and use such vulnerabilities to their advantage (Caldwell, 2012).

The SolarWinds breach is acknowledged as one of the largest cybersecurity breaches in recent history (Alkhadra et al., 2021). Discovered in 2020 this attack targeted SolarWinds, a leading provider of IT management software impacting approximately 300,000 major organizations across key sectors like military and government. Human error played a role in the breach through the use of the software update process that allowed malicious code to integrate into the updates. The intrusion went unnoticed for months due to oversights in following security procedures at levels. Moreover, the choice of a password, like "solarwinds123" which was later exposed online, indicates a failure to enforce strict password regulations. The incident involving SolarWinds serves as an example that human errors are not limited to mistakes, but also involve how organizational guidelines support or fail to address these errors effectively.

A study by Alaskar et al. (2015) emphasizes the significant challenges organizations face in aligning formal information security (IS) processes with the actual behaviors of their employees. Despite having developed frameworks and comprehensive IS policies focused on protecting organizational data and systems, there is often a noticeable disparity between these established policies and the way employees interact with these systems on a daily basis. A key concern highlighted is the lack of adherence among employees who may not fully comprehend or value the importance of these security protocols. The report indicates that a considerable number of organizations believe that their employees have a poor understanding of their IS policies. This lack of understanding can lead to security breaches and vulnerabilities, despite the presence of policies and guidelines designed to mitigate these risks. Reflecting on the practical challenges of enforcing these standards, recent studies have identified a significant gap between the theoretical frameworks provided by information security standards and their actual implementation within organizations (Lundgren and Bergström, 2019; Niemimaa and Niemimaa, 2017; Njenga and Brown, 2012; Siponen, 2006; Siponen and Willison, 2009). According to these studies, although these standards outline necessary security processes, they often do not address how these processes should be effectively implemented in real world scenarios.

1.1 Problem Definition

Given the significant role that human errors play in security breaches, as evidenced by recent statistics and research, it is crucial to focus on the roles and responsibilities within an organization. The absence of defined roles and responsibilities can contribute to these human errors of employees. Höne and Eloff (2002) highlight the role of roles and responsibilities in information security standards, stating that they are components of a strong security framework. This perspective is supported by studies that emphasize the importance of defining roles and responsibilities in improving an organization's security posture (Bulgurcu et al., 2010; Choi et al., 2018; Lowry and Moody, 2014; Singh and Gupta, 2017). However, there is still a significant gap in the literature when it comes to determining whether security policies are adequately established and effectively define roles and responsibilities. Furthermore, there has been insufficient research on the alignment of these policies with real employee practices. This discrepancy can increase human errors and violations of security protocols, especially if employees do not fully understand the rationale behind the policies (Choi et al., 2018). The existing literature points to significant gaps in the implementation of information security measures (Lundgren and Bergström, 2019; Niemimaa and Niemimaa, 2017; Njenga and Brown, 2012; Siponen and Willison, 2009), indicating that despite the recognized importance of clearly defined roles and responsibilities, organizations may struggle to effectively implement these strategies. There is a need in gaining insight into how well organizations adhere to advised standards and frameworks regarding the implementation of roles and responsibilities to enhance security measures. This problem definition addresses the practical gaps between theoretical security policies and their actual implementation within organizations. Hence, exploring whether standards and regulatory frameworks that govern roles and responsibilities are being fulfilled and whether they are adequate in their current state is important. The focus is on uncovering the discrepancies between intended policies and real-world practices, investigating the reasons behind these discrepancies, and the challenges that employees face due to unclear roles and responsibilities.

1.2 Aim and Objectives

The study aimed to investigate the discrepancies between defined security policies and their actual implementation concerning roles and responsibilities within organizations. One key objective was to identify where established security policies differ from their practical application in roles and responsibilities. This includes analyzing how security measures are implemented and identifying discrepancies. The study also aimed to discover the reasons for these gaps, such as unclear guidelines or policy misinterpretations, contributing to observed disparities. This study has strategically chosen a case company within the highly sensitive and regulated Swedish defense industry to explore these implementation gaps more deeply. A company as such operating in the defense industry is expected to adhere strictly to security protocols and standards (Timmermans, 2022; Nordlund, 2022). This study examines a high-stakes setting to determine if security standards are truly adhered to or if significant discrepancies exist between the documented policies and their actual implementation. findings from this case study are crucial for understanding the effectiveness of security practices in environments where compliance must be beyond reproach, offering insights into how roles and responsibilities are managed in critical sectors that operate on both national and international stages. To fulfill the research aim and its objectives, the following research questions was defined to be answered:

Q1 What are the discrepancies between defined security policies and their actual implementation concerning roles and responsibilities?

Q2 What are the underlying reasons for these gaps in the implementation of security policies?

1.3 Research Structure

In subsequent chapters, we will explore the implementation of security policies within organizational roles. Chapter 2 provides a comprehensive background, covering relevant preliminaries and prior research to contextualize the study. After reviewing the relevant concepts and literature, Chapter 3 introduces the chosen research methodology, detailing the approach and methods used. Chapter 4 presents the result while Chapter 5 outline the analysis of the results, highlighting the discrepancies in the implementation of the policy. Chapter 6 will discuss in detail the reasons behind the identified gaps and the contribution

to previous research. Lastly, Chapter 7 provides a summary of key insights, recommendations, and suggestions for future research.

2 | Background

This chapter lays the foundation for the rest of the study by introducing and explaining key ideas, theories, and research that has previously been conducted. There are two subsections to this chapter: "2.1 Preliminaries" and "2.2 Research Background." The first subsection outlines important terms and concepts that are needed to understand the study. The second part looks at previous research to put this study in the context of larger academic discussions. The goal of this chapter is to provide readers with a broad background to understand the deeper topics discussed in this study.

2.1 Preliminaries

In this first main section of the background, essential concepts, theories, and frameworks are presented to help readers understand the following study content. Key definitions and core principles have been outlined to ensure that all readers can understand the important elements discussed in the study, regardless of their level of familiarity with the subject matter.

2.1.1 Information Security

Information serves as a way of sharing knowledge and is integral to daily living, being communicated, stored, processed, and transmitted in various forms (MSB, 2015). Information can be in digital or analog format, including text, visuals, or audio (Nieles et al., 2017). Information security is about protecting this information and the systems that handle it from various threats. According to the National Institute of Standards and Technology (NIST), information security is *"protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability"* (Nieles et al., 2017). Similarly, the International Organization for Standardization (ISO) defines information security as *"protection of confidentiality, integrity, and availability of information"* (ISO/IEC, 27001, 2022). Both standards highlight the importance of confidentiality, integrity, and availability, known as the CIA triad (ISO/IEC, 27001, 2022; Nieles et al., 2017). As illustrated in Figure 2.1, the CIA triad is essential to information security, *Confidentiality* ensures that only authorized individuals can access information. *Integrity* involves ensuring the accuracy and reliability of the information. *Availability* ensures that information is accessible when needed (ISO/IEC, 27001, 2022; Nieles et al., 2017; Nikander et al., 2020).

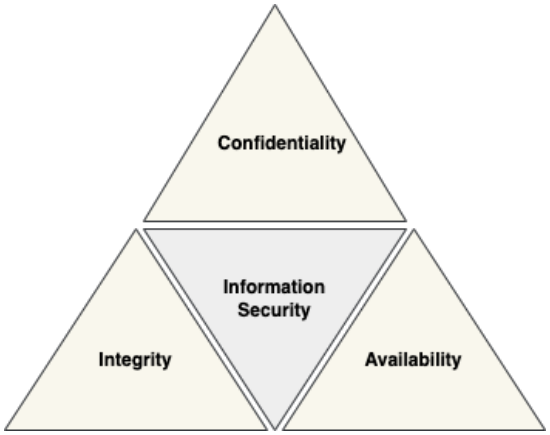

Figure 2.1: Representation of the CIA triad (Author's own)

It is important to clarify the use of the terms *"information security"* and *"cybersecurity"* in this study, as the terms are often interchangeable. Information security refers to protecting data in all its forms, be it digital or physical (Taherdoost, 2022). This means protecting information contained in written documents as much as protecting information stored in a database. Cybersecurity, on the other hand, focuses on defending the organization against cyberattacks and any other cyber incident security. Cybsersecurity therefore focuses on protecting digital information stored in digital media such as computers, servers, and digital documents, making cybersecurity considered a subset of information security as seen in 2.2. This study directly relates to information security, as it involves analyzing how security measures are applied in practice within organizations and identifies the gaps and the reasons behind these gaps. These investigations are also crucial for cybersecurity because they improve defenses against security breaches caused by human errors or policy misinterpretations.

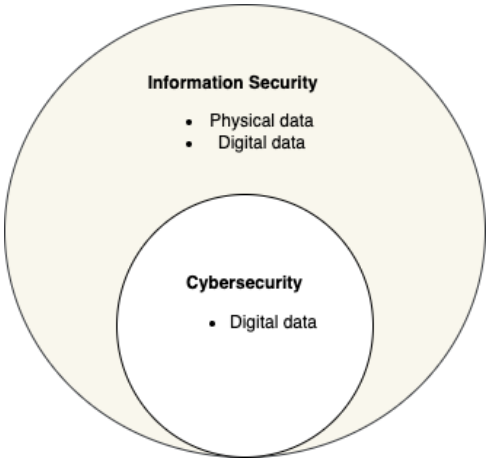

Figure 2.2: Distinction between Information Security and Cybersecurity (Author's own)

2.1.2 The Human Element

Emphasizing the human element and organizational commitment in upholding the CIA triad principles highlights that information security extends beyond technology to include people who interact with systems and data (Ashenden, 2008; Costantino et al., 2018; Stewart and Jürjens, 2017). The approach to information security threats in organizations has been based mainly on technology(Singh et al., 2014; Bulgurcu et al., 2010), focusing on the implementation of technical solutions to protect systems against unauthorized access, data breaches, and other cyber threats. This technical focus assumes that strong security technologies and systems alone can adequately protect organizations from potential risks. However, recent studies have highlighted a critical shift in this perspective (Ashenden, 2008; Bulgurcu et al., 2010; Costantino et al., 2018; Singh et al., 2014; Stewart and Jürjens, 2017), underscoring the impor-

tance of considering human factors alongside technological measures. Costantino et al. (2018) explore vulnerabilities introduced through social engineering attacks, which exploit human psychology rather than system weaknesses. This study illustrates that technological safeguards alone are insufficient if individuals within the organization can be manipulated to compromise security protocols. Adding to this discussion, Ashenden (2008) points out that the management of information security is a larger challenge that involves more than just technology and processes; it includes the effective management of people. The study argues that organizational culture, the identity of security managers, and effective communication are critical factors that have often been overlooked but are essential for a robust information security strategy. Despite these insights, many organizations continue to invest heavily in technological solutions without equally prioritizing the human elements of information security (Soomro et al., 2016). This unbalanced focus makes them vulnerable to non-technical aspects of security threats, such as insider threats, social engineering, and simple human error.

In 2015 according to Gehem et al. (2015) 95% of all security breaches attributed to human error, nine years later, this statistic persists, remaining at 95% (Hancock and Tessian, 2022). This means that human error remains one of the primary causes of security breaches in information systems and has remained consistently high and unimproved over nearly a decade. Stewart and Jürjens (2017) identifies human error in information security as actions or behaviors of employees that violate company security policies or directly contribute to security breaches. These according to Stewart and Jürjens often arise from underlying problems such as poor security awareness, lack of proper information security training, negligence or carelessness such as sharing passwords or clicking on malicious link, and poorly managed teams or lack of clear management directives. The study by Stewart and Jürjens (2017) suggests that these human errors are an important risk factor for information security and should be addressed through better training, enhanced security policies, and a culture of security awareness within the organization.

2.1.3 Information Security Management

To assist organizations in safeguarding their information security two essential frameworks are introduced; Information Security Management (ISM) and Information Security Management Systems (ISMS) (Haufe et al., 2022; Zammani and Razali, 2016). ISM focuses on overseeing information according to the principles of the CIA triad, employing policies and procedures to protect against threats (Zammani and Razali, 2016). On the other hand, ISMS is a framework that aims to put ISM into action, manage it effectively, and improve by incorporating policies, procedures, and controls to address security risks (Haufe et al., 2022). It follows standards such as ISO/IEC 27001 to ensure that security measures are implemented in an organized manner according to practices. By implementing ISMS, organizations can manage their information security in a way that aligns with their business goals and meets requirements efficiently. ISMS serves as the structured infrastructure to operationalize ISM, ensuring that all critical safeguards are in place and work effectively to protect information assets. Essentially, ISM outlines information protection, while ISMS offers a systematic framework for its effective implementation and management.

Based on the knowledge that effective ISM goes far beyond technological measures to include human aspects, it is essential to explore the role and importance of information security policies (ISPs). ISPs are critical organizational documents that outline the responsibilities of all stakeholders regarding the security of all information assets. These policies provide a framework for setting expectations, defining roles, and specifying the technology and methods to enforce security controls within an organization(Kadam, 2007; Solms and van Niekerk, 2013; Peltier et al., 2003). These policies are critical to ensure that information remains secure, confidential, and available, as well as to ensure the integrity of data. They serve as guidelines for information security management and help in risk management by defining the roles and responsibilities of individuals, specifying security measures, and setting the standards for compliance and security controls. An information security policy defines and prioritizes the organization's security objectives, along with detailing the tactics and security measures in place to protect digital and physical information assets. These policies are essential because they create a formal standard against which all activities are measured, ensuring consistency in security enforcement. Such policies are crucial not only for protecting sensitive information from external threats, such as hackers and cyberattacks, but also from internal threats, such as accidental breaches or misuse of data. As mentioned above, information security is not just about technology; it also involves the human aspect, such as employee behavior and adherence to policies. Therefore, it is important for the ISP to be relevant to the business, align with

recognized security frameworks, and be measurable against internal and external standards (Andress and Leary, 2017). It should cover various aspects, including data confidentiality, integrity, availability, and compliance with relevant laws and regulations (Photopoulos, 2008).

According to Höne and Eloff (2002), it is pointed out that security policies often do not really impact employees because they are not aware of them, find them too complicated to comprehend, or see them as irrelevant to their daily activities. As a result, employees can ignore security measures, viewing them as inconvenient rather than essential. Höne and Eloff argument that for an information security policy to be effective, it should not just have the right content, but also be communicated in a way that captures the employees interest and shows its relevance to their work. Bulgurcu et al. (2010) emphasizes the importance of having clearly defined roles and responsibilities in the ISP. By clearly stating what employees are expected to do, organizations can better align employee behavior with organizational security objectives.

2.1.4 Roles and Responsibilities

According to Höne and Eloff (2002) it is crucial to have a defined and effectively communicated approach to the roles and responsibilities of information security. They stress that for an information security policy to be truly effective, it must be clearly defined and embraced by all employees in the organization. This means that roles and responsibilities should be effectively communicated so that users not only know about them, but also understand how their actions impact information security. Building on this Choi et al. (2018) point out the significance of having defined roles and responsibilities to strengthen an organizations information security posture. They highlight the importance of aligning security objectives with the organization's mission to protect information assets and ensure that employees understand what needs protection. Furthermore, Singh and Gupta (2017) underscores the role of defined roles and responsibilities in bolstering an organization's information security posture. He emphasizes that a comprehensive information security policy that describes roles, responsibilities, and expectations forms the foundation for the implementation of security measures at organizational levels, from senior management to operational staff. These studies highlight the need to define roles and responsibilities to ensure policy compliance and detect protocol violations.

ISO/IEC 27001

ISO/IEC 27001 is a leading standard in information security (Culot et al., 2021), offering a framework for organizations to develop, implement, maintain, and enhance their ISMS. Adherence to ISO/IEC 27001 enables organizations to manage risks, safeguard sensitive information, and show their commitment to best practices in information security. The ISO /IEC 27001:2022 standard, which has been updated from the 2013 version (Malatji, 2023), addresses new technological and security challenges. Understanding the difference between ISO/IEC 27001 and ISO/IEC 27002 is important. ISO/IEC 27001:2022 provides the framework for managing information security and risks (Suorsa and Helo, 2024), and ISO/IEC 27002:2022 guides the implementation of specific controls within this framework to meet the security objectives. The two standards work together to ensure holistic and effective management of information security within the organization. Both standards stress the importance of clearly defining roles and responsibilities to ensure that all employees understand their roles in securing information assets. Control 5.3 in ISO/IEC 27001:2022 describes the role of top management in governing information security and stressing their responsibility by indicating that top management must:

- Assign and communicate responsibilities and authorities for relevant roles within the organization.
- Ensure that the ISMS complies with the stated requirements.
- Take accountability for reporting on the ISMS's performance.

Although ISO/IEC 27001 establishes the framework, ISO/IEC 27002:2022 provides actionable guidance on implementing this framework by detailing the roles and responsibilities necessary to maintain information security (Suorsa and Helo, 2024). ISO/IEC 27002:2022 also advises on the competency requirements of individuals in security roles, the need for ongoing education, and the importance of clear accountability in delegating security tasks. Control 5.2 in ISO/IEC 27002:2022 specifies the following:

- Information security roles and responsibilities should be established, approved, and understood within the organization to manage and protect information effectively.

- Specific responsibilities include the protection of information, the execution of security processes, risk management, and ensuring that all personnel are responsible for using the organization's information assets securely.

Both ISO/IEC 27001 and ISO/IEC 27002 work together to enhance the security stance of organizations by establishing a framework for accountability and ownership. They guarantee clarity regarding roles and responsibilities, minimizing the chances of security breaches caused by misunderstandings or negligence.

NIST

NIST, a non-regulatory agency of the US Department of Commerce, develops standards and guidelines to advance technology and promote innovation (NIST, 2024). Its Cybersecurity Framework (CSF) helps organizations assess and enhance their capabilities to prevent, detect, and respond to cyber threats. Widely recognized and used worldwide, the CSF is noted for its comprehensive and flexible approach suitable for various organizational sizes and sectors (Sayed et al., 2023). It serves as a foundational element in many cybersecurity programs and is endorsed by governments, industry bodies, and professionals. Rohan et al. (2023) notes that the CSF effectively strengthens cybersecurity by aligning human factors, reducing incidents and breaches.

The CSF identifies a category called *GV.RR - Roles, Responsibilities, and Authorities* as a component of successful cybersecurity governance (NIST, 2024). This category emphasizes the necessity of setting clear standards for who is responsible for what, who has decision making authority, and how these responsibilities are communicated across the organization. According to GV.RR, individuals and teams must understand their respective responsibilities. Establishing and defining these roles, responsibilities, and authority promotes accountability and openness inside the company. Everyone understands their duties and knows who to contact for specific cybersecurity concerns, which improves coordination and reaction times to security incidents. Furthermore, it provides effective performance evaluation and continuous development by allowing businesses to monitor the efficiency of people and teams in carrying out their cybersecurity obligations. The GV.RR category in the NIST-CSF emphasizes the need of clearly defining and communicating an organization's roles, responsibilities, and authority in order to encourage accountability, improve performance, and strengthen cybersecurity.

2.2 Research background

In this second main section of the background offers an overview of several studies examining the implementation of information security policies and frameworks in organizational contexts. The section discusses critiques of existing standards and guidelines, challenges in integrating security practices into organizational workflows, and gaps between theoretical frameworks and practical realities in policy compliance.

2.2.1 Standardized Policies to Practical Implementation

A study by Siponen (2006) focuses on the limitations of widely used information security management standards. The main argument presented is that these standards tend to ensure only the existence of certain security processes or activities within organizations without sufficiently addressing how these processes should be implemented effectively; they focus on whether something is done rather than how well it is done. Siponen's analysis highlights a significant gap between the policy writing (the standards) and its practical implementation. He points out that, while these standards are good at listing required security activities, they fail to guide how to execute these activities effectively to achieve the intended security outcomes. This disconnect can cause organizations to have a false sense of security simply by following the standards without effectively securing their systems. To address these issues, Siponen (2006) discusses examples from various standards to illustrate how they often provide vague guidelines that do not translate into practical, actionable advice. For example, standards might require organizations to train employees in security procedures without specifying what effective training should look like or how to motivate employees to follow these procedures. Ultimately, the study calls for future standards and research to pay more attention to the content and quality of security processes, rather than just their existence. Siponen (2006) suggests that more in-depth case studies and action research are needed to understand how security standards can be better implemented in practice to truly secure

organizational systems. Building on this critique, the study by Siponen and Willison (2009) extends the discussion by examining the "one-size-fits-all" approach of ISM guidelines such as BS7799 and ISO/IEC 17799. They argue that these universal standards do not meet the specific security needs of different organizations. Moreover, they point out that the validation of these standards typically relies on expert consensus or common practice rather than empirical evidence, which may not accurately reflect their effectiveness in various real word environments. To overcome these issues, Siponen and Willison (2009) propose a change in the way ISM guidelines are developed. They advocate for an empirical approach where guidelines are rigorously tested and validated through scientific research to ensure that they effectively enhance security. This would allow for the customization of guidelines according to specific organizational needs and contexts. In addition, they suggest restructuring the ISM guidelines from rigid and prescriptive rules to a library of research-based security practices. This library in their means would provide a diverse range of strategies, tools, and principles, all supported by evidence of their effectiveness, from which organizations could select to best meet their unique security challenges. The combined insights from both of these studies (Siponen, 2006; Siponen and Willison, 2009) call for ISM standards to be adaptable, empirically validated, and practical, offering not just a framework for compliance but robust guidance for achieving genuine security resilience. This approach according to the authors would not only bridge the gap between theoretical policy writing and effective implementation but also foster a more security conscious culture within organizations where security measures are understood, respected, and effectively implemented by everyone involved.

The theme of adapting security practices to specific organizational realities is further explored in the study by Niemimaa and Niemimaa (2017). The authors used an ethnographic approach to closely observe and analyze the implementation of information system security (ISS) policies in a real world setting. They studied how an IT service provider translated the best practice of ISS information classification into an ISS policy and into situated practices. This involved detailed observations and interactions with participants, providing a deep, contextual understanding of the policy implementation process. Central to their findings, the authors emphasize the necessity of addressing existing nonstandard, informal practices within organizations, which they term "non-canonical practices". The authors point out that these practices may deviate from formal policies and pose security risks, therefore making it important to reconstruct these practices to align them with the intended security objectives. This detailed study highlights the dynamic and iterative process of policy implementation, underscoring the importance of adapting security practices to the lived realities of organizational life. By delving deep into the daily operations and the specific contextual challenges faced by an IT service provider, the authors illustrate how abstract ISS guidelines often fall short unless they are effectively integrated into the specific workflows and cultural nuances of an organization. Their work points out that for ISS policies to be truly effective, they must not only be adapted to the organizational context but also actively reshaped by the daily practices and interactions of the employees. This research offers valuable insights into the complexities of policy implementation in the realm of information systems security, providing scholars and practitioners with a deeper understanding of how to bridge the gap between theoretical best practices and their practical applications.

Lundgren and Bergström (2019) echo these concerns by showcasing the discrepancies between the formal, linear descriptions of ISRM processes and their real word applications. The study reveals that in real word scenarios, there are notable differences between these formal descriptions and how ISRM is actually implemented day-to-day. ISRM processes are often depicted in formal organizational policies and standards typically present ISRM as a linear sequence of steps, where tasks like information classification, risk analysis, and implementation of security controls are shown to progress seamlessly from one to the next, without much consideration for the dynamic and complex nature of real word scenarios. As a consequence, the implementation of ISRM in practice involves more negotiation, adaptation, and improvisation than formal policies typically acknowledge. This means that practitioners often have to navigate complex social dynamics and organizational structures to effectively manage information security risks, which can deviate significantly from the straightforward processes outlined in formal policies. This is emphasized in a study by Njenga and Brown (2012) that highlights the discrepancies between the way policies are typically written and implemented and the realities faced by ISS practitioners. The study observed that there are often situations where existing security policies do not fully cover or address immediate challenges or threats. In response, security practitioners tend to rely on improvisation to adapt and overcome these challenges effectively and fill the gaps left by formal policies. Both studies (Lundgren and Bergström, 2019; Njenga and Brown, 2012) suggest that this gap between policy formulation and

implementation is due to formal policies that typically assume stability and predictability in information security environments. However, the dynamic reality of security threats requires a more adaptable and improvisational approach to the formulation and implementation of policies.

2.2.2 Practical Challenges in Security Policy Integration

The concept of integrating security practices into the daily workflows of organizations is argued by Niemimaa (2016). Niemimaa critiques the traditional view of ISM as a linear process aimed at strict adherence to standards like ISO/IEC 27001. She introduces a 'practice lens' framework to offer a more realistic perspective on managing information security in organizations. Employing an ethnographic approach, she immersed herself in the daily operations of an IT service provider. This method provided deep insights into the practical challenges of implementing information security policies. Through her observations, Niemimaa identified a challenge in the integration of security practices into daily work routines, which are often seen as burdensome by employees who do not perceive these tasks as part of their core responsibilities. The employees also shared the feeling that their perspectives and concerns are not considered in the formulation of security policies and perceived the policies as disconnected from their daily work realities. In addition, conflicts often arise between the prescribed security policies and the actual needs and practices of the organization. These conflicts highlight a discrepancy between what is outlined in security policies and the practical realities of organizational operations. Such misalignment can hinder effective implementation and adherence to security measures. Essentially, she suggests that these policies should be designed to be more flexible and responsive to the specific context in which they will be implemented. To achieve effective implementation, Niemimaa (2016) emphasizes the importance of engaging stakeholders throughout the policy development process. This ensures that the policies are not only theoretical but also practical and relevant to the employees who will be responsible for implementing them. In essence, Niemimaa research advocates a shift in how organizations approach information security management. By adopting the practice lens, they can better understand the interaction between organizational culture, social interactions, and security practices. This understanding can lead to the development of security management strategies that are not only more effective in achieving compliance, but are also seamlessly integrated into the daily activities and cultural fabric of the organization, thereby enhancing overall security posture.

Alaskar et al. (2015) add to the conversation by addressing the difference between how IS policies are supposed to work in theory and how employees actually use them. Even though organizations have well thought out theoretical frameworks and detailed policies to protect their data and systems, the study showed that there's often a gap between how employees actually use these formalized measures in their daily work. One big problem is that many employees don't fully understand how important these security measures are, so they don't follow them. Even when strict rules are in place, this lack of understanding can lead to breaches and weaknesses that were not meant to happen. Alaskar et al. argues that different factors affecting employee compliance have been researched, but they haven't been put together in a way that makes sense to effectively guide employee behavior. This means that many IS policies haven't changed, even though technology and the ways people use and share data in the modern workplace are changing quickly. Since these policies don't change, they might not be able to keep up with new threats or changes in technology. This could according to Alaskar et al. cause a gap between the policies in place and the organization's real security needs. The study suggests using strategies for ongoing education and communication to deal with this problem. These strategies should be made to keep employees up to date on the newest security risks and best practices. They should also be made to fit the problems that employees face at work. Companies can help close the gap between policy and practice and improve overall information security by constantly training their workers and keeping them up to date on how security is changing. The authors state that it's not enough to have well thought out policies; these policies must also be communicated to employees in a way that they understand and be easily incorporated into their daily work. In a related study Bulgurcu et al. (2010) discusses the challenges organizations face in ensuring compliance with their Information Security Policy (ISP) among employees. They emphasizes that while ISPs are designed to guide employees in securing data and managing sensitive information, there's often a significant disparity between these policies and what actually happens in practice. This gap can be attributed to factors like employees lack of awareness about the policies, the inconvenience they perceive in following them, and a belief that strict adherence might impede efficiency. The study stresses the importance of employees complying with ISPs to reinforce organizational information security. It highlights that employees' understanding and acceptance of their responsibilities outlined in

the policies are crucial for their effectiveness. Moreover, the study explores how employees make decisions regarding ISP compliance, considering factors such as the perceived benefits and costs. It suggests that emphasizing the benefits of compliance and the costs of non-compliance can help align employees' behaviors with the formal roles and responsibilities set out by ISPs.

2.3 Contribution

Although previous studies (Alaskar et al., 2015; Bulgurcu et al., 2010; Lundgren and Bergström, 2019; Niemimaa, 2016; Niemimaa and Niemimaa, 2017; Njenga and Brown, 2012; Siponen, 2006; Siponen and Willison, 2009) have highlighted the gap between theoretical policy formulations and their actual application in organizational contexts, there is still a notable gap in literature regarding the significance of clearly defined roles and responsibilities in ensuring effective security measures. Given the significant role that human errors play in security breaches, it is crucial to focus on the roles and responsibilities within an organization. The lack of clear and well implemented roles and responsibilities can be a major factor contributing to these human errors (Caldwell, 2012; Hancock and Tessian, 2022; Stewart and Jürjens, 2017; PwC, 2015). Unlike previous studies that may broadly examine policy implementation across various organizational contexts, this study aims to contribute by providing a detailed empirical analysis that explores how security policies are implemented, with a specific focus on roles and responsibilities within the Swedish defense industry. Because of the critical nature of its operations and the potential consequences of security breaches, this sector with high security stakes is expected to follow rules and regulations strictly (Nordlund, 2022; Timmermans, 2022). Therefore it serves as an excellent case study for examining not only discrepancies between policy and practice but also the reasons behind these discrepancies. Academically, by conducting research in a critical sector and presenting empirical evidence, the study adds depth to theoretical models of ISM and information security strategy (ISS), offering nuanced insights into how security policies are put into practice. Furthermore, the findings of this research have the potential to inspire the development of new theoretical frameworks or improvements to existing ones, especially to understand how to structure roles and responsibilities to effectively strengthen security measures. This contribution is important for academia because it expands the empirical foundation upon which security management theories are built and provides a solid basis for future research, especially in areas where security is of utmost importance. These contributions as seen in Figure 6.1 are vital for academics and practitioners alike, as they provide a more grounded basis for designing security policies that effectively reduce human errors and enhance overall security resilience.

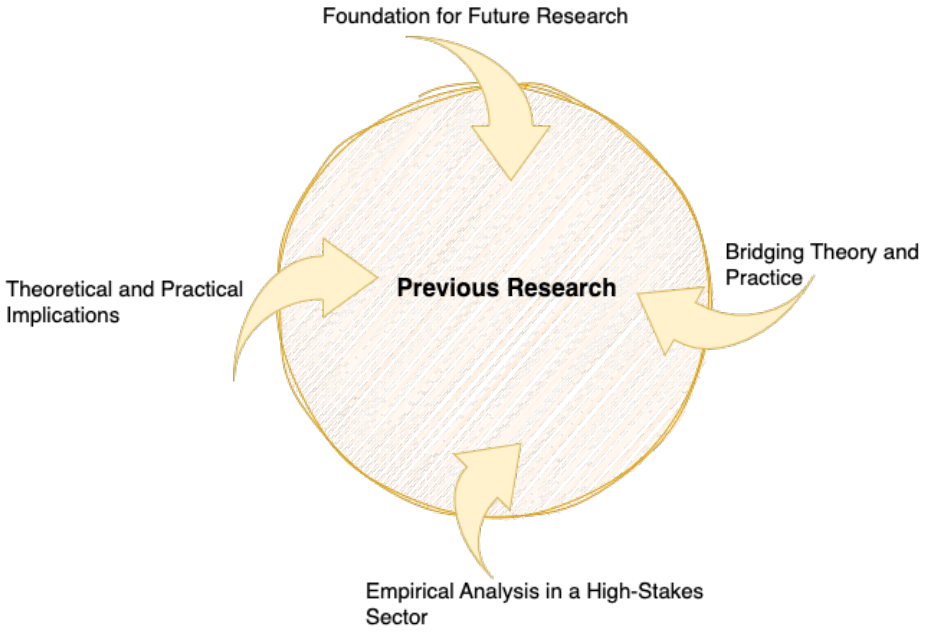

Figure 2.3: Contribution to Existing Research (Author's own)

3 | Method

This chapter presents the chosen research methodology, describes the qualitative research approach, and emphasizes the particular techniques for data collection and analysis. Furthermore, this section describes the approaches taken to guarantee the reliability and validity of the results and explains why these approaches were chosen. The delimitation and ethical issues raised by the implementation of the methodological approach are also discussed.

3.1 Research Design

This study used qualitative research methods, including a case study approach, to better understand the discrepancies between theoretical security policies and their practical implementation. By focusing on roles and responsibilities, it explores how these roles are defined, communicated, and executed, which are often not easily quantifiable. According to Steckler et al. (1992), qualitative research seeks to reveal deep insights into human behavior, experiences, and perceptions by asking questions about the "how" and the "why". This makes it ideal for exploring how employees understand and implement security standards in their daily operations. This research uses a case study to investigate the implementation of security policies within the internal software supply chain of a Swedish defense company, a case company. Gerring (2004) describes a case study as a qualitative research method focused on analyzing a specific example within its real life context. This method provides detailed insight into complex issues and helps to understand the underlying reasons behind actions and events. It also allows for the examination of differences between planned strategies and actual outcomes, highlighting the complexities and variations in real word scenarios.

3.1.1 Selection of Case Company

The choice of a Swedish defense company as the case company was strategic, driven by its significant role within the highly regulated defense sector, which demands strict adherence to security protocols (Nordlund, 2022; Timmermans, 2022). This company is not only a leader in the industry, but also represents a typical entity that faces the challenges of implementing theoretical security policies practically. This setting is ideal for investigating the discrepancies between defined security policies and their actual implementation, directly aligning with the study's aim and objectives outlined in Section 1.2. In addition, the selection of this company was influenced by its accessibility and willingness to participate in academic research, which is crucial to conducting in-depth qualitative investigations. The company's widespread operations offer a valuable perspective on the implementation of security policies across various levels and locations, highlighting the complexities in a global context. Due to the sensitive nature of the information involved and the high stakes associated with security practices in the defense sector, the company's identity will be kept confidential and anonymous throughout this study. This measure ensures the protection of proprietary and sensitive data while allowing for a detailed exploration of the subject matter. The context of this case company allows for a detailed analysis of security practices and the identification of gaps between policy and practice, addressing the research questions defined in Section 1.3. By examining such a critical player in the defense industry, the study aims to contribute valuable findings on the effectiveness of security practices in environments where compliance is non-negotiable.

3.2 Data Collection

The main research tool was semi-structured interviews, which were considered ideal for this type of case study because they provided a structured but flexible approach to data collection (Mathers et al., 1998). This method allowed for in-depth exploration of how theoretical security policies were applied practically while ensuring that all relevant aspects of policy implementation were consistently covered throughout the interviews. Semi-structured interviews allowed for the collection of detailed descriptions of the processes, challenges, and outcomes associated with the implementation of security policies, with a focus on roles and responsibilities. It explored how these roles were defined, communicated, and executed. By allowing interviewees to express their thoughts in their own words while also guiding them to discuss specific areas of interest, these interviews provided a rich and qualitative understanding of the current state of policy application. Using open-ended questions (Mathers et al., 1998), semi-structured interviews offered flexibility in questioning, allowing interviewers to follow up on interesting leads and investigate for further insights in real time. For example, questions such as "Can you describe a typical day in your role within the software supply chain?" or "What challenges do you face when implementing security policies in your daily tasks?" encouraged participants to elaborate on their experiences and insights. Open-ended questions also provided the flexibility to delve deeper into specific areas based on participant responses, resulting in a richer understanding of the challenges and gaps in practice.

Interview Setup

The interviews were conducted and recorded remotely using Skype, the company's primary platform for meetings and communication. This choice was taken in consideration of the company's expansive global presence, operating across various sites worldwide, including several locations in Sweden. Remote interviews enabled participation in these diverse geographical locations, including those working from home. In addition, it simplified the interview scheduling process, particularly given that many were now working from home and preferred remote meetings. One of the advantages Skype offered was screen sharing, both interviewers and participants were able to have interactive discussions by sharing visual aids when needed. However, it was important to note that a disadvantage of not having face-to-face interviews is that you may not be able to use body language and other nonverbal signals in the same way (Mathers et al., 1998). Nevertheless, Skype as a platform provided a good compromise by offering the ability to see each other in real-time, thereby facilitating a more personal interaction even at a distance.

Each interview was assigned an 60-minute slot allowing time for in-depth discussions without feeling rushed. The recording of each interview ensured comprehensive data for analysis (Mathers et al., 1998), adhering to company policies by storing recordings exclusively on the company's computer systems in accordance with security protocols. All interviews were conducted in Swedish, which was the local language of the participants. Participants were offered to choose between Swedish and English beforehand and all participants chose Swedish as the language with which they were most comfortable. The idea behind letting participants choose the language they preferred was to gather genuine and detailed responses, since participants could express themselves more freely (Welch and Piekkari, 2006). This not only made the collected data more valuable but also adhered to qualitative research principles, which emphasize understanding the context and deeply engaging with the perspectives of the participants.

Interview Guide

The interview guide consisted of open-ended questions to enable in-depth discussions and was structured around several key areas that included:

1. **Definition and Clarity**: The questions explored how roles and responsibilities were defined within the organization. This included investigating whether these definitions were clear, accessible, and comprehensible to all employees involved, especially in relation to IT security within the software supply chain.

2. **Communication Effectiveness**: This area assessed how roles and responsibilities were communicated between different levels of the organization. The questions aimed to determine the effectiveness of these communication methods and whether they adequately supported employees in understanding and executing their duties.

3. **real word Implementation**:Questions dug into the actual application of defined roles and responsibilities in daily operations. This included exploring any discrepancies between formal policies and their practical implementation, which could highlight areas of misalignment that affect security measures.

4. **Challenges and Improvements**: Identify specific challenges that employees faced due to potential ambiguities or inefficiencies in role definitions and responsibilities. The questions also invited suggestions for improvements, providing actionable insights based on real world experiences.

The interview guide was presented in Swedish and had also been translated into English for greater accessibility. Appendices A and B contained the original Swedish version and its English translation, respectively. It should be noted that the original guide was in Swedish, reflecting its use in interviews conducted in the local language. Appendix B featured the English translation, although it was not a literal translation but one that closely mirrored the essence of the questions, ensuring the capture of their intended meaning.

Sampling Method

A qualitative research as mentioned seeks to gain insight through first-hand experiences of individuals involved in the study context (Mathers et al., 1998; Hammarberg et al., 2016). It was not feasible to conduct the study on an entire population and, therefore, the need to sample the selection of a subset of participants from a larger population (Makwana et al., 2023). There are several types of sampling techniques, and in this study, a purposive sampling approach was chosen. Purposive sampling is where the researcher determines the required information and selects individuals with the necessary knowledge or experience willing to provide it (Etikan et al., 2015). In the context of this study, purposeful sampling was used to select individuals who were involved in different roles within the management of the company's software supply chain, as seen in Table 3.1. Each process in software supply chain management was led by a designated department and has a process leader. The procurement department, for example, was responsible for choosing and assessing software providers where a process leader was assigned to supervise these activities. This leader led the process of evaluating vendors, negotiating contracts, and making sure the chosen vendors met the company's requirements. Process leaders were chosen for this study for purpose because they are the ones in charge of managing the processes involved in the management of the software supply chain. In the event that a process leader was unavailable, they were asked to suggest a participant with similar experience within the same process to ensure a representative sample of participants.

The decision to select participants from various departments within the software supply management aimed to achieve a comprehensive overview of the entire chain of interest. This approach was beneficial for several reasons. First, by including participants from different departments, a diverse range of perspectives and experiences related to the implementation of security policies could be captured at various stages of the software supply chain. Secondly, involving individuals from different parts of the internal software supply chain allowed the examination of the interconnections of roles and responsibilities within the organization, highlighting potential areas of alignment or divergence in policy interpretation and application.

Table 3.1: Roles of Respondents in Software Supply Chain Management (Authors own)

Respondent	**Role**	**Experience (Year)**
R1	Head of IS/IT - Procurement	7
R2	Service Owner - IT Security	15
R3	IT manager - Provide Third-party Software	2
R4	Process Leader - Export Control	3
R5	Process Leader - Procurement	5
R6	Compliance Manager	6
R7	IT Security Specialist	2
R8	Process Leader - Quality Management System (QMS)	12
R9	Process Leader - Accreditation	3
R10	Process Owner - Incident Response	5

Sampling Size

The determination of the appropriate sample size for this investigation was based on the saturation principle (Hennink and Kaiser, 2022), a method that is frequently used in qualitative studies to ensure a sufficient depth of data. Saturation is reached when the additional data collection no longer produces a new understanding relevant to the research questions, suggesting that the data set is comprehensive enough to support a robust analysis. The interview process was conducted until the tenth interview, at which point no new themes or valuable insights emerged, indicating that saturation had been achieved. This threshold is in line with established research that indicates that saturation often occurs after 9 to 17 interviews, which according to Hennink and Kaiser (2022) depends on the homogeneity of the study population and the scope of the research questions. Therefore, as seen in Table 3.1, insights were collected from 10 respondents, Respondent 1 to Respondent10.

3.3 Data Analysis

Given the importance of the semi-structured interviews in the data collection strategy, careful consideration of the data analysis technique was required from the beginning to ensure that the data was appropriately captured and examined.

3.3.1 Thematic Analysis

In this study, thematic analysis was employed to examine the qualitative information gathered from semi-structured interviews. As noted by Braun and Clarke (2006), thematic analysis is a flexible technique that is widely accepted in qualitative research for *identifying, analyzing, and reporting patterns, or "themes," within data.* The benefit of theme analysis's flexibility is that it lets the data itself, rather than preconceived frameworks, shape the analysis. This is very helpful for studies like this that look at a variety of subjective experiences and points of view. The ability to analyze the overwhelming and complex nature that is often associated with large volumes of data is another benefit of thematic analysis, as it helps the researcher approach data analysis methodically (Braun and Clarke, 2006). According to Braun and Clarke, a theme *"captures something important about the data in relation to the research question, and represents some level of patterned response or meaning within the data set"*. Themes that represent the diverse experiences and attitudes present in the dataset are essentially used to identify topics that encapsulate the essence of the data. In this instance, the transcribed interview responses from the study's conducted interviews make up the dataset.

Within thematic analysis, there are two approaches to identifying themes within the data: inductive and theoretical (Braun and Clarke, 2006). Theoretical thematic analysis can be described as research-driven, focusing more on predetermined frameworks, while inductive thematic analysis is data-driven. In this context, predetermined frameworks refer to ideas, themes, or categories that a researcher may have formed before examining actual data. These frameworks are based on previous knowledge, theories, or assumptions about what the data might reveal. In other words, they are preexisting structures that the researcher brings into the analysis process. Using predetermined frameworks can influence how the data is interpreted because the analysis might be directed towards confirming these existing ideas rather than allowing new insights to emerge naturally from the data. This approach can sometimes restrict the depth of understanding because it may overlook unexpected patterns or themes that do not fit into predetermined frameworks. The inductive approach to thematic analysis avoids predetermined frameworks by starting the analysis without fixed ideas about what will emerge. This allows the themes to develop naturally on the basis of the data itself. Such an approach is valuable when exploring complex or poorly understood phenomena, as it can lead to a more genuine and comprehensive understanding of the data, capturing a wider range of experiences and perspectives that might otherwise be missed. Since the aim is to uncover how roles and responsibilities are defined, communicated, and executed within the organization, starting without predetermined frameworks allows the data to speak for itself. This can lead to a more authentic and grounded understanding of the internal dynamics and real world challenges in policy implementation. As illustrated in 3.1 , the thematic analysis process involves several systematic steps as described by Braun and Clarke. Braun and Clarke (2006).

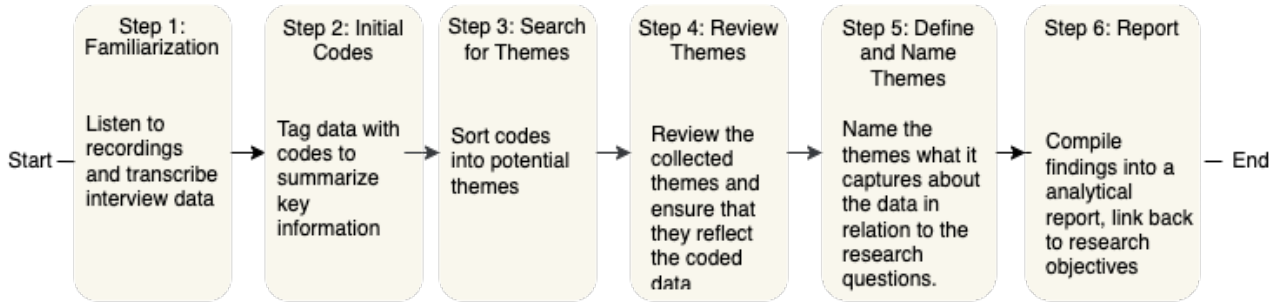

Figure 3.1: The process of thematic analysis (Author's own)

Step 1: Familiarization

The analysis began with the transcription of each interview, conducted verbatim to capture the complete content of the discussions. The familiarization process involved three thorough readings of these transcripts, the first was to gain a general sense of the information without making any formal notes. During the second reading, initial impressions, thoughts, and potential patterns were noted to identify how the data might relate to the research questions. The final reading focused on beginning to develop a coding scheme. Attention was paid to recurring themes, phrases, and feelings expressed by the participants relevant to their experiences with the clarity and communication of the role.

Step 2: Initial Codes

Following familiarization, the systematic coding of the data ensued. This entailed identifying text segments that captured key thoughts or concepts relevant to the research questions. Initial codes such as "Clarity of Role and Process Definitions," "Role Ambiguity and Challenges," and "Formality vs. Practicality in Descriptions" were applied. This coding process was iterative, allowing for modifications and refinements as new patterns emerged.

Step 3: Search for Themes

Following familiarization, the systematic coding of the data ensued. This entailed identifying text segments that captured key thoughts or concepts relevant to the research questions. Initial codes such as "Clarity of Role and Process Definitions," "Role Ambiguity and Challenges," and "Formality vs. Practicality in Descriptions" were applied. This coding process was iterative, allowing for modifications and refinements as new patterns emerged.

Step 4: Review Themes

The themes were reviewed to ensure an accurate representation of the coded data and the entire dataset.This review involved refining the themes, ensuring that they were distinct but comprehensive enough to encapsulate the related data points. Some themes were merged, others split, and some were discarded on the basis of their relevance and coherence with the dataset.

Step 5: Define and Name Themes

Once the themes were established, they were clearly defined and named. The definitions were designed to clearly communicate the scope of what each theme covered and the names were chosen to reflect the essence of the underlying findings.

Step 6: Report

The final report was drafted by selecting illustrative quotes from the transcripts that best demonstrated the themes. These quotes were used to enrich the narrative and provide empirical evidence for the analysis. The thematic analysis report was structured logically, introducing each theme and supporting it with quotes from the data, ensuring clarity and coherence in presenting the research findings in Chapter 4. Following this, Chapter 5 will go into a detailed analysis of these findings.

3.4 Reliability and Validity

According to Golafshani (2003), reliability in research means that the results remain consistent over time and accurately represent the entire population being studied. This principle entails that the research can be repeated with the same outcomes, validating the credibility of the results. In simpler terms, a study is reliable if it produces consistent findings when the research methods are repeated or if different researchers conduct the study under similar conditions. Reliability in this research is enhanced by:

- **Structured Interviews**: These interviews have a basic structure but also allow for deeper exploration of topics that come up during the conversation. This approach helps ensure that every interview covers similar ground, which supports consistency across different sessions.
- **Recording and Language Use**: All interviews are recorded and conducted in Swedish, the primary language in Sweden where the participants are based. This reduces the chance of losing important details or misunderstanding what is said, helping ensure that the data collected are accurate and consistent.
- **Purposive Sampling**: The selection of participants through purposive sampling is designed to include individuals directly involved with or knowledgeable about the internal software supply chain and security policies. Choosing participants specifically because they have direct experience or knowledge about the topic ensures that the information gathered is relevant and consistent.

On the other hand, validity depends on how reliable and solid the study findings are (Golafshani, 2003). Validity means checking whether the study actually measures what it is supposed to measure and if the conclusions drawn are logically supported by the evidence collected. Validity ensures that the research results make sense and can be applied to the real word situation they are aimed to represent. Validity is addressed in the study through:

- **Rich, Detailed Data Collection**: Semi-structured interviews make it possible to gather comprehensive, situation-specific data. This approach is beneficial because it allows participants to provide in-depth insights into their real-world experiences, which is essential to understand how policies are implemented in practice.
- **Semi-structured Interviews**: Semi-structured interviews allow participants to freely communicate their ideas and experiences due to their flexibility. Since the information is obtained directly from those responsible for carrying out the security policies, this approach improves the accuracy of the data.
- **Thematic Analysis**: Analyzing the data through thematic analysis helps identify genuine patterns and themes from the conversations. By letting these themes emerge naturally from the data rather than imposing any predefined ideas, the analysis remains closely tied to what the participants stated, enhancing the validity of the study.

3.5 Delimitation

Delimitations are boundaries, "limits" that the researcher sets to define the scope of the research (Theofanidis and Fountouki, 2019). In this study, the following delimitations were established:

- **Research Focus:** Focusing only on a Swedish military business allows for a thorough examination of specific cases and instances where security policies may conflict with practical implementation. This concentration gives in-depth insights into certain organizational behaviors and decision-making processes, but it may limit the capacity to apply these results to other industries or cultural situations. Understanding how roles and responsibilities are formed, communicated, and carried out in this particular setting gives information on distinct organizational dynamics, but it may not reflect differences present in other organizational environments.
- **Qualitative Methodology**: The qualitative methodology, particularly case studies and semi-structured interviews, is ideal for investigating the "how" and "why" of security policy implementation. It highlights the realities of human behavior and the complexity required in policy implementation that quantitative data may overlook. However, this method often provides context-specific and subjective outcomes, which may not be easily replicated in other settings or provide the breadth of data that quantitative data could provide with.

- **Purposive sampling:**
  - **Targeted Expertise and Relevance:** Purposive sampling ensures that participants have direct experience or are significantly involved in the roles and processes relevant to the study's aim. This approach guarantees that the data collected are rich in detail and directly pertinent to the study's focus on security policy implementation discrepancies. However, by focusing only on individuals who are expected to have the necessary expertise, the study can exclude other stakeholders within the organization who could provide additional perspectives on the broader impact of security policy or other related issues. This could include junior employees, other departments, or even external partners who interact with company security measures, but whose insights might differ from those more directly involved in policy management.
  - **Depth Over Breadth:** This sampling method allows an in-depth exploration of complex issues from the viewpoint of those most knowledgeable and responsible. Although this provides depth, it does not necessarily allow for a broader overview of how security policies are perceived and implemented throughout the organization. Therefore, the study findings are limited to the experiences and perspectives of a selected group of individuals, which may not capture the full range of experiences and could affect the generalizability of the conclusions.
  - **Bias Towards Certain Roles:** Focusing on process leaders and other key managerial roles ensures that the information collected reflects a high level of oversight and responsibility concerning security policies. This selection bias might overlook the operational realities faced by employees who deal with the day-to-day implementation of these policies, but who are not in leadership positions. The nuances of how policies are executed on the ground, potential discrepancies experienced by junior employees, and informal adaptations or misunderstandings that occur in practice might be underrepresented.
- **Geographical Scope**:
  - **One Case Company:** Focusing on a Swedish defense company offers a detailed look at security policy in a regulated sector, highlighting the unique challenges of strict security protocols. Sweden's strict regulations enhance the study's relevance, but limit its broader applicability due to unique defense practices and regulatory norms that may not align with other sectors or regions.
  - **Local Context:** Although the company is global, the study focuses primarily on Sweden, which could overlook variations in the implementation of policy in other operating countries. This focus may not capture the influence of local cultural, economic, or legal factors on the application of security policy outside Sweden.
  - **Operational Environment:** The specialized nature of the defense sector, with its unique operational demands and security requirements, means that the findings might not be easily transferable to less regulated or different types of industries. The operational practices, employee roles, and security measures specific to the defense sector may differ considerably from those in other sectors, such as retail, education, or healthcare.

3.6 Ethical Considerations

Because qualitative research involves close contact between participants and researchers (Kyngäs et al., 2020; Mack et al., 2005), ethical issues are crucial and frequently involve the gathering of private and sensitive data. From data collection to publication of results, researchers must protect participant privacy and personal information (Kyngäs et al., 2020). The main goal of a study is always the well-being of the participants, claims Mack et al. (2005). When researchers have to decide between endangering the research or participants, the safety of the participants has to come first. Kyngäs et al. (2020) emphasizes as additional significant components of research ethics responsibility and openness in the research process. For the public to accept and respect research, its techniques, procedures, and findings must be easily available and transparent. In qualitative studies delving deeply into human experiences, in particular, researchers can protect their subjects and improve the quality and trustworthiness of research by rigorously following certain ethical principles. In this study, theoretical security measures were applied in practice in a sensitive setting, and therefore following ethical guidelines was very important. Several fundamental ideas directed the ethical framework of the study:

Informed Consent and Voluntary Participation

Participants were thoroughly informed about the study's purpose, what it entailed, and the use of the data collected. They were also assured of their right to withdraw from the study at any point, ensuring that participation was entirely voluntary. This process respects the autonomy of the participants and is fundamental in qualitative research, where the depth of personal insight and experiences can have significant personal implications.

Anonymity and Confidentiality

Protecting the identities of participants and the confidentiality of the data collected is especially critical in a defense context where information sensitivity is paramount. Anonymity was guaranteed to all participants to prevent any personal or professional repercussions, and data were stored within the company's internal network and was securely stored to further ensure the integrity and security of the information.

Sensitivity and Impact

Given the potential implications of the research findings on security practices and policy, the research was conducted with responsibility and consideration for the broader impact of the findings. Discussions and recommendations were framed in a way that supports positive changes without compromising current operational integrity.

Potential Bias

The purposive sampling strategy employed for the selection of the study participants was strictly based on their professional roles and responsibilities, based only on their professional roles and responsibilities, not on their gender, age, race, or any other factor that could be considered biased. This sampling strategy helped promote fairness and reduce the risk of discrimination and unfair influence in participant selection. By focusing on the professional functions of participants within the company, the study avoids introducing biases that could skew the data and interfere with the objective analysis of how security policies are enacted in practice. This approach ensures that the findings reflect systemic practices and insights specific to the roles critical to company security operations, rather than being influenced by irrelevant personal characteristics of participants.

4 | Result

This chapter of the study presents the results of the thematic analysis, the results of the data analysis process are presented, detailing how individual observations were categorized into codes and then grouped into broader themes. These themes emerge from the analysis and provide a structured understanding of the data based on the study's research questions and framework.

4.1 Thematic Coding

During the thematic process described in 3.3.1, individual observations and information pieces were labeled with precise descriptive codes. As patterns emerged, similar codes were combined to reduce redundancy and highlight significant trends. Codes that shared underlying themes were grouped under a combined code. The combined codes were then elevated to broader themes, representing overarching issues or concepts present in the data. The decision to group certain combined codes into a single theme was driven by the study's overarching research questions and theoretical framework. For example, the combined codes related to the ambiguities and practical challenges of role execution informed the creation of a theme like *Challenges in Role Clarity and Responsibilities*. Table 4.1 visually maps out the hierarchical relationship between the specific codes, the more general combined codes, and the overarching themes. This structure illustrates the analytical journey from the specificity of individual codes to the broader understanding encapsulated in the themes.

Table 4.1: The structural approach of coding to themes (Author's own)

Theme	**Combined Code**	**Codes Covered**
Formal Roles and Practical Realities	Formal vs. Actual Role Discrepancies	Formality vs. Practicality in Descriptions, Reality vs. Formal Role Descriptions, Inefficacy of the current platform Workday, Discrepancy in Role Implementation and Compliance, Gap Between Role Descriptions and Practice
Challenges in Role Clarity and Responsibilities	Role Ambiguity and Transition Challenges	Role Ambiguity and Challenges, Lack of Formal Role Definition, Need for Role Clarification Amid Rapid Growth, Challenges Due to Unclear Roles, Challenges with Role Descriptions for Transitions, Junior Employees Struggle with Ambiguity
Communication of Roles and Responsibilities	Role & Responsibility Communication and Clarity	Informal Role Communication, Sufficient Role Communication, Communication of Roles and Responsibilities
Role Flexibility and Individual Adaption	Role Flexibility and Personalization	Role Adaptation and Freedom, Flexibility in Role Fulfillment, Self-Designed Role, Role Clarity and Guidelines
Enhancing Role Clarity	Practical Improvements for Role Definitions	Suggested Improvement for Clarity, Improvements in Role Definitions, Role Descriptions in Practice

4.2 Findings

In this thematic analysis, insights were collected from a diverse group of participants, labeled Respondent 1 (R1) through Respondent 10 (R10), and chosen as described in 3.2. Thematic analysis revealed five main themes, each encapsulating critical aspects of the discrepancies between formal role descriptions and practical realities within the organization.

It should be noted that the interviews revealed two different systems used for role management within the company: the Global Management System (GMS) and Workday. In GMS, role descriptions are associated with individuals who either have a placeholder role within a specific process or who are responsible for overseeing ("owning") a process. Participants who are not part of any process in GMS do not have a defined role or description within this system. For those not included in GMS processes, their job descriptions are maintained in Workday.

4.2.1 Formal Roles and Practical Realities

In the thematic analysis of semi-structured interviews, a significant discrepancy between formal role descriptions and the actual responsibilities and practices experienced by employees was repeatedly highlighted. Participants expressed concerns about the formalization of roles that do not translate into practical, actionable guidelines.

Table 4.2: Respondent Quotations on Formal Roles and Practical Realities

Respondent	Quotation
R1	"I believe that a role description becomes very very formal and a process description also becomes very formal, it does not really tell us how we should implement it in real life."
R3	"The role and description I have on Workday are not really reality, I do not have the same role and responsibility in reality as I have on Workday."
R8	"Another problem is that the workday where we are supposed to have our roles and responsibilities defined is only used for classifying employees and the role descriptions are not really the reality and that is a problem."
R6	"The reality is that currently only those individuals with a placeholder role in GMS have defined roles and responsibilities. The rest of us who work in daily operations and may not necessarily own a process do not have defined roles or responsibilities. My reflection is that external demands are imposed on us, and we simply do things to demonstrate compliance without truly understanding that it applies to the entire organization, not just what the organization prioritizes as important."
R2	"The platform Workday where we have somewhat a description of our role and responsibilities have actually no meaning."
R9	"There is always a discrepancy because somewhere you have to adapt it to reality and we are all different individuals who will focus on different parts of the role description."

4.2.2 Challenges in Role Clarity and Responsibilities

Some respondent underscored the critical need for clear defined roles and responsibilities to maintain organizational efficiency and effectiveness. Clear definitions of roles help reduce misunderstandings, improve employee morale, and ensure that all organizational processes run smoothly. Especially as organizations scale, maintaining clarity in roles becomes essential to manage complexity and ensure that all team members understand their specific contributions to the organization's goals.

Table 4.3: Respondent Quotations on Challenges in Role Clarity and Responsibilities

Respondent	Quotation
R1	"We often find ourselves in situation where we do not know who is responsible for what, take accreditation for example, who is responsible for driving the process and make sure it has been done? Is it us? Is it them?"
R7	"I find that my role and responsibilities lack clear definition, as they are primarily communicated by my manager through expectations and tasks. I find it sometimes challenging because it leaves room for misunderstanding and confusion."
R7	"Sometimes you hear people complain about doing another colleagues work, which they see as beyond their responsibility, and then they get frustrated with their colleagues. In my opinion, that frustration might be because we do not really know each other's responsibilities."
R2	"Our team, now consisting of 70 people, has undergone rapid growth, and unfortunately, we haven't quite managed to finalize the puzzle of defining our roles and responsibilities. Frankly, we need to establish our delivery process before we can achieve clarity in roles and responsibilities within the team."
R4	"We once had an issue where a software update was ready for release, but the export compliance checks were not thoroughly completed due to a misunderstanding about who was responsible for the final review."
R10	"Handing over responsibilities smoothly is a challenge, when there is no predefined role description to guide the process. Without a clear understanding of what is expected, it is easy for important tasks and information to fall through the cracks during the transition."
R7	"There are several of us who are juniors and I notice that we have a need to have clear roles and responsibilities, we struggle to understand what is expected of us."
R8	"For someone who has worked in an area for quite some time, it is very clear, but if I can be objective, if someone junior or new comes into the role, it is not easy to interpret what the role description actually means in practice."

4.2.3 Communication of Roles and Responsibilities

This theme reflects on the way roles and responsibilities are conveyed within organizations, identifying both the obstacles encountered and the successful strategies employed to foster understanding and effectiveness among employees.

Table 4.4: Respondent Quotations on Communicating Roles and Responsibilities

Respondent	Quotation
R4	"I learned my roles and responsibilities through experience, when I started, I did not get a description of what my role is and what my responsibilities are, but somehow I managed through it by talking to my manager who communicated these responsibilities to me."
R5	"Today we communicate the roles and responsibilities with each other, we tell each other what the expectations are, and we keep track of who in the team is responsible for what."
R7	"Another situation is that there was a reorganization and I got a new manager and then a completely new responsibilities based on the new manager's expectations were communicated to me."
R6	"The reality is that currently only those individuals with a placeholder role in GMS and own a process have defined roles and responsibilities. The rest of us who work in daily operations and may not necessarily own a process do not have defined roles or responsibilities. My reflection is that external demands are imposed on us, and we simply do things to demonstrate compliance without truly understanding that it applies to the entire organization, not just what the organization prioritizes as important."

4.2.4 Role Flexibility and Individual Adaption

In this theme participants discussed the balance between having defined roles and the freedom to adapt these roles to suit individual strengths and preferences. The following responses underscore the importance of balancing clearly defined role expectations with the flexibility to adapt roles to individual capabilities and circumstances.

Table 4.5: Respondent Quotations on Role Flexibility and Individual Adaptations

Respondent	Quotation
R5	"Sometimes without role descriptions like me, having too much freedom in your role can backfire. You might start to wonder if you are on the right track, if your priorities are in order, or if you have the right responsibilities. You don't know where you are or what is expected of you; it is like wandering around without a compass".
R10	"Different people are good at different things, so someone might spend 50% of the time on a responsibility in their role description, while another person in the same role spends 5% on the same responsibility."
R10	"Our department started 2.5 years ago and I have had the opportunity to design my own role and its definition, and maybe that is why I don't really have a problem with the role description".
R3	"I was involved in defining my role and responsibilities, and therefore for me it is clear what my role and responsibilities are".
R3	"We don't really need stricter roles and responsibility descriptions, I like and find ways to do things, as long as I adhere to important rules, I prefer to do it my way".

4.2.5 Enhancing Role Clarity

Participants offered various suggestions on how role descriptions could be improved to better serve their practical needs and clarify daily responsibilities.

Table 4.6: Respondent Quotations on Enhancing Role Clarity

Respondent	Quotation
R1	"Instead of all that formal language, why not write them more like we are having a chat? Like, imagine explaining your role to a friend over coffee, It would be way easier to understand, right? We could make them clearer and more straightforward for everyone so that there is no confusion about who is supposed to do what. Just a thought, but I think it could really make a difference."
R5	"Role descriptions these days sometimes feel more like job postings than clear guidelines on what we are supposed to do. It is like they throw in all these expectations about our skills and knowledge, like how good we need to be at English, when really, that is not what a role description should be about. It should focus on what we are responsible for and who we are supposed to work with, not whether we can ace an English exam."
R8	"You know, it's crucial to make sure everyone's responsibilities are clear, but sometimes those role descriptions get so big they're like trying to hold onto a handful of sand. It is just hard to keep it all together and know exactly what you are supposed to do. Maybe we could break things down a bit, you know? Like, chop those big roles into smaller pieces with clear jobs and goals for each part. That way, we all know what we're doing without getting lost in the big picture. It's about finding that balance between covering everything we need to and making sure we can actually handle it all effectively."
R9	"We need role descriptions that actually mean something in our day-to-day work, not just a big chunk of text that leaves us scratching our heads. We should be able to look at our responsibilities and know exactly what we need to do, step by step. Like, what does it actually mean for me to follow up on my responsibilities? That's what we need to make crystal clear. Let's make it practical, break it down into real-life scenarios or tasks so we can all hit the ground running and get stuff done without feeling lost in our roles."
R6	"We should have a system where we can see our roles and responsibilities, not just written down to look good and comply with various frameworks and regulations. Role descriptions should reflect reality."

5 | Analysis of Result

The themes provided a comprehensive understanding of the multifaceted challenges and dynamics experienced by employees in various roles. The Swedish defense company, although it is compliant with ISO/IEC 27001 and NIST 800-171 and maintains an ISMS as recommended by these standards, exhibits notable discrepancies. These standards stress the importance of clearly defined policies for roles and responsibilities. However, the findings suggest that these are not adequately implemented or reflected in actual practices within the company. The discrepancies between the formal roles as defined by the organization and the practical realities of their execution are significant. In theory, roles and responsibilities within the Swedish defense company are clearly defined in documents such as role descriptions and security policies. However, in practice, employees often find themselves navigating ambiguities and adapting their roles to meet the immediate demands of their tasks. This misalignment is evident in several areas, as seen in the analysis in Figure 5.1.

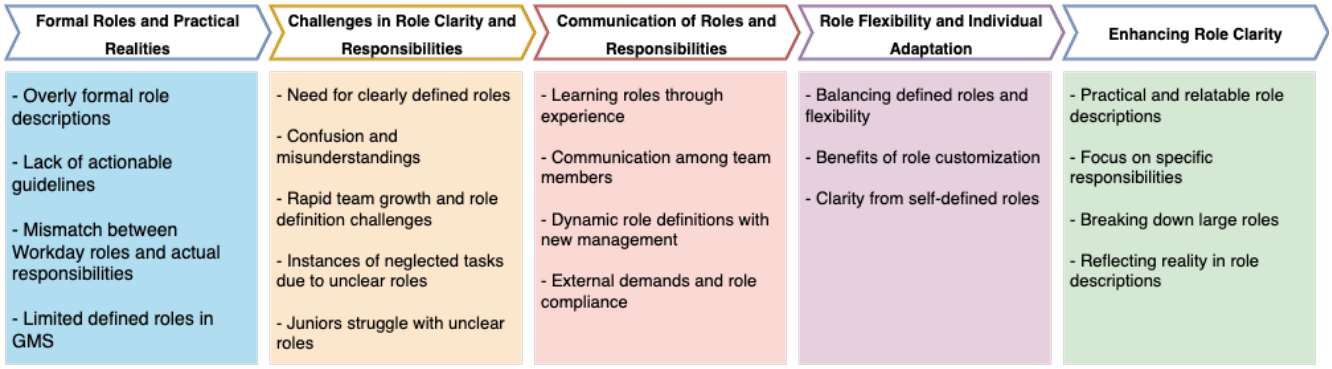

Figure 5.1: Analysis of the themes (Author´s own)

5.1 Formal Roles and Practical Realities

A major finding is the substantial gap between formal role descriptions and the actual responsibilities employees experience. The organization uses two systems for role management: GMS and Workday. GMS associates role descriptions with individuals who hold a placeholder role within a specific process or oversee a process. In contrast, Workday maintains job descriptions for those not included in GMS processes. Respondents found that formal role descriptions overly rigid and not reflective of real-life responsibilities. For instance, R1 noted that role descriptions are very formal and lack actionable guidelines, while R3 and R8 pointed out that their roles in Workday do not match their actual responsibilities. R6 emphasized that only those with placeholder roles in GMS have defined responsibilities, leaving others to perform tasks to meet external demands without a true understanding of their roles. Additionally, R2 stated that their Workday role descriptions have no practical meaning, and R9 added that adapting role descriptions to real-world scenarios is necessary as each individual focuses on different aspects of their role.

5.2 Challenges in Role Clarity and Responsibilities

Respondents underscored the critical need for clearly defined roles and responsibilities to maintain organizational efficiency and effectiveness. Ambiguity in roles leads to misunderstandings and frustration. R1 highlighted situations where it was unclear who was responsible for specific tasks, such as accreditation. R7 mentioned that their role and responsibilities lacked clear definition, causing confusion and misunderstandings. R2 pointed out the challenge of defining roles within a rapidly growing team of 70 people. R4 and R10 shared instances where critical tasks were neglected due to unclear role definitions, such as a software update delayed by a misunderstanding over export compliance checks. R7 also noted that juniors struggle to understand what is expected of them without clear roles, while R8 observed that experienced employees find role definitions clearer than newcomers.

5.3 Communication of Roles and Responsibilities

Effective communication of roles and responsibilities is vital for employee understanding and performance. Current communication methods vary, with some employees relying on managers' expectations and peer discussions. R4 described learning roles through experience, while R5 mentioned that they communicate roles and responsibilities among team members to manage expectations. R7 noted that the responsibilities changed with a new manager, highlighting the dynamic nature of the definitions of the roles. R6 reiterated that only those with defined roles in GMS have clear responsibilities, while others comply with external demands without a complete understanding. This variation in communication methods points to the need for consistent, clear communication strategies to ensure that all employees have a mutual understanding of their roles.

5.4 Role Flexibility and Individual Adaption

Some Respondents valued the ability to adapt roles to their strengths, but too much freedom can lead to uncertainty. R5 mentioned that without clear role descriptions, excessive freedom can cause confusion and self-doubt about one's responsibilities and priorities. In contrast, R10 found the opportunity to design their own role beneficial. R3 appreciated the clarity of participating in defining their own role, while another R3 preferred less strict roles to allow personal initiative.

5.5 Enhancing Role Clarity

Respondents offered various suggestions for improving role descriptions to better serve practical needs and clarify daily responsibilities. R1 proposed to write role descriptions in conversational language to make them more relatable. R5 and R9 emphasized that role descriptions should focus on specific responsibilities rather than broad qualifications, noting that overly detailed descriptions can be overwhelming. R8 suggested breaking large roles into smaller, manageable parts to avoid confusion. R6 emphasized the need for role descriptions that reflect reality rather than complying with regulations.

6 | Discussion

This section interprets the findings and their implications, examining how they align with existing research and theories, the impact of the methodology, and exploring alternative interpretations. It also assesses ethical and societal considerations to understand the broader implications of the research comprehensively.

6.1 Theoretical Framework

This section evaluates how the findings of this study enrich the understanding of existing theories in information security, focusing particularly on role clarity and responsibilities within high-risk environments. For a visual summary of the intersections and divergences between previous research and this study's contributions, see Figure 6.1

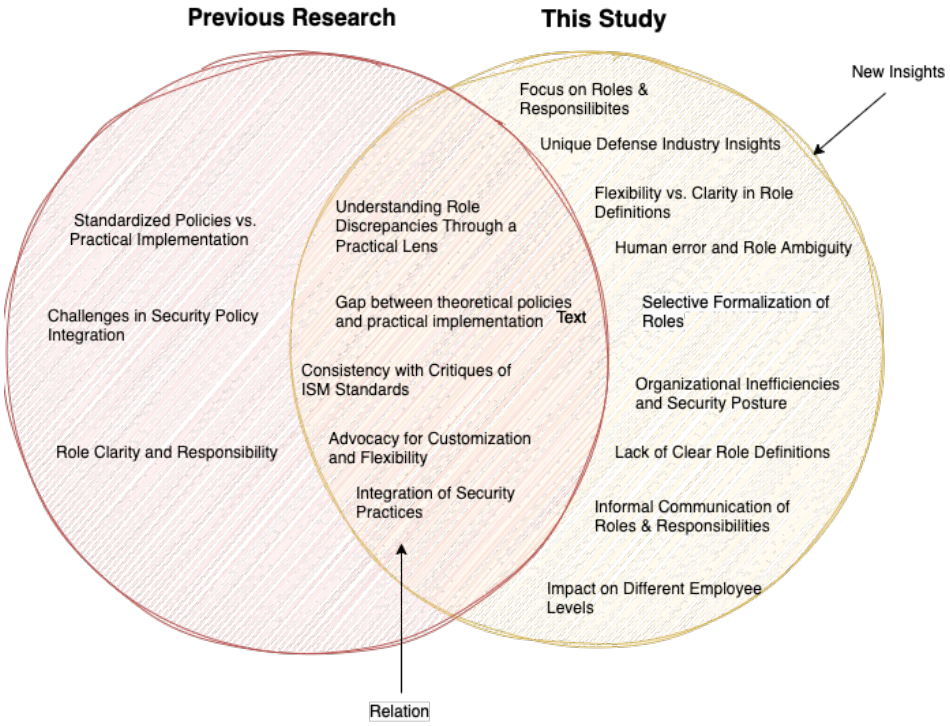

Figure 6.1: New Insights to Existing Research (Author's own)

6.1.1 Relation to Previous Research

As seen in Figure 6.1 this study emphasizes the consistent gap between theoretical policies and their practical implementation, reflecting the concerns noted in earlier research. It underscores discrepancies between defined roles and actual responsibilities within organizations, reflecting common themes in information security management (ISM) and organizational role implementation studies. The findings

highlight a pervasive issue: theoretical frameworks do not always align with practical applications, especially concerning organizational roles and security practices. Such misalignments were also criticized by Siponen (2006), who argued that standards often fail to ensure effective implementation, merely confirming the existence of processes. Participants in this study describe their roles as excessively formalized, which hinders practical operations. This ineffectiveness underscores the need for ISM guidelines to focus not only on establishing procedures but also on their practical efficacy, advocating a change from formality to functionality. Siponen and Willison (2009) suggested customizing the ISM guidelines to meet the unique needs of different organizations, a point supported by the findings on the flexibility of the role in this study. This flexibility has led to improved job satisfaction and effectiveness, highlighting the inadequacy of a one-size-fits-all approach. Furthermore, the study aligns with Niemimaa and Niemimaa (2017), emphasizing the integration of security practices into daily workflows to improve clarity and operational efficiency. The real-world application of these theories reveals that role descriptions often do not reflect the dynamic nature of actual responsibilities, leading to ambiguities that affect both operational effectiveness and engagement with security practices.

6.1.2 New Insights to Previous Research

Prior studies had generally critiqued ISM standards for their theoretical focus and lack of practical applicability, emphasizing the need for security practices adaptable to specific organizational contexts. However, the focus on the Swedish defense sector and the specific challenges of software supply chain management differentiated this study from previous research. It not only bridged the theoretical gaps identified in previous studies but also provided a detailed understanding of the unique challenges faced by organizations operating within these specific contexts. The study dived deeply into a specific organizational context, revealing that discrepancies in role clarity and the formalization of role responsibilities directly impacted security practices within the Swedish defense industry. It provided detailed examples of how formal role descriptions often did not reflect the actual duties employees performed, which often led to confusion and operational inefficiencies. Employees, especially those in junior positions, faced significant challenges as they were expected to interpret and adapt these formal descriptions to the practical demands of their roles. This situation was exacerbated by the findings that some roles did not even have clearly defined responsibilities and expectations, leaving employees to navigate their tasks based on informal communication and personal judgment. Moreover, the study highlighted the lack of integration of formal security practices into the daily responsibilities of employees. The current study built on this by providing concrete examples in which the lack of clear role definitions and the informal manner in which roles were communicated led to significant discrepancies between what was prescribed by security policies and what was actually practiced. This misalignment not only affected junior employees who struggled with unclear expectations but also resulted in broader organizational inefficiencies and a weakened security posture (Alaskar et al., 2015; Niemimaa and Niemimaa, 2017). Previous research had recommended that role definitions within information security management should be flexible to better accommodate the specific needs and contexts of different organizational environments. This approach, according to these studies, was beneficial because it allowed employees to adapt their roles to the dynamic challenges and requirements of their specific tasks, which was believed to improve engagement and effectiveness. However, the current study within the Swedish defense company's software supply chain management offered a different perspective. Some respondents indicated that too much flexibility in roles could lead to confusion and inefficiencies. They noted that excessive freedom in role definitions often left them questioning their exact responsibilities, leading to uncertainty about whether their priorities and actions were aligned with organizational goals. This sentiment reflected a challenge where too much flexibility could lead to a lack of clarity and consistency (Siponen and Willison, 2009).

6.2 Methods, Implementation and Results

The methods employed in this study, particularly thematic analysis, allowed for a comprehensive exploration of the discrepancies between formal role descriptions and practical realities within the Swedish defense company.

Impact of Selected Method

By conducting semi-structured interviews and thematically coding the data, this study was able to identify five main themes that encapsulated critical aspects of these discrepancies. The thematic analysis

provided valuable insights into the challenges and dynamics experienced by employees in various roles, which might not have been as apparent using a more quantitative approach. Such a methodological choice ensured that the complexities of human behavior and organizational culture's impact on policy implementation were adequately captured and analyzed.

Alternative Interpretations of Results

The results suggest a significant gap between prescribed roles and actual practices, which could be interpreted as either a failure in policy communication or as an indication of the need for more adaptive policy frameworks. This gap might also reflect the dynamic and complex nature of security environments where formal policies cannot comprehensively cover all scenarios encountered by employees. Another interpretation of the findings concerns the existence of roles without clear descriptions, even though the company holds certifications and maintains an established ISMS. This discrepancy can be interpreted as potential weaknesses in the certification processes themselves or in how the standards are applied within the organization.

General Applicability of Results

While the findings are specifically relevant to the Swedish defense sector, they highlight a common issue that could apply to various sectors, especially those involving complex security management systems. The insights gained could therefore be beneficial for organizations aiming to enhance their information security management by aligning formal policies more closely with practical, on-the-ground challenges.

Implications for Practical Activities

In practical terms, the results underscored the importance of clear and effective role definitions within organizations, particularly in complex environments such as the defense sector. They highlighted the potential consequences of role ambiguity, including inefficiencies, misunderstandings, and operational challenges. To address this, organizations could revise role descriptions to make them more flexible and directly relevant to the daily tasks of employees. This would help bridge the gap between policy expectations and reality, making them more practical and easier to follow in real world scenarios and enhance the security posture.

6.3 Ethical and societal aspects

The implementation of the study's findings on managing roles and responsibilities within information security, especially within the context of the Swedish defense sector, raises important ethical and societal considerations if applied to the real world. The considerations are also related to the relevant United Nations Sustainable Development Goals (SDG) (United Nations, 2024).

Ethical Considerations

- **Fairness in Role Assignment**: Roles must be assigned equally and fairly so that all employees understand their responsibilities without feeling overwhelmed. According to Inuwa (2017) a fair distribution of roles promotes morale and productivity. There is a risk of subjective bias in the assignment of roles, which can result in discrimination or unequal distribution of workload. Ensuring fairness and equality in role assignment contributes to the reduction of workplace inequalities, which is consistent with SDG 10.
- **Privacy and Data Protection**: In defining roles clearly, organizations may need to monitor tasks and employee performance, raising concerns about surveillance and privacy. Protecting individual privacy and ensuring data protection help to build fair and peaceful societies, reinforcing SDG 16's emphasis on promoting peaceful and inclusive societies for sustainable development.
- **Bias and Discrimination**: There is always the possibility that biases in role definition will lead to discrimination, whether intentionally or unintentionally. To ensure diversity and inclusion, role definitions must be created with no bias based on age, gender, ethnicity, or any other factor. Actively preventing bias and ensuring without prejudice practices in role assignment and management contribute to SDG 5, which aims to achieve gender equality and empower all women and girls, as

well as SDG 10, which focuses on reducing inequalities based on gender, age, ethnicity, and other statuses.

Social Impacts

- **Transparency and Trust**: Applying the study's findings could result in clearer definitions of roles within organizations, which can increase operational transparency. This transparency can boost trust among employees by helping them understand their responsibilities, as well as among external stakeholders, such as consumers and regulatory bodies, who can see that the organization is well organized and accountable. However, too much transparency could disclose critical information, especially in a military context, which could be misused if intercepted by unauthorized parties. Clear responsibilities and transparent processes help to develop accountable and inclusive institutions, which is one of SDG 16's primary objectives.
- **Employee Well-being**: Clearer role definitions can improve employee well-being by reducing ambiguities that often lead to stress and confusion at work. This clarity allows employees to better understand their specific duties and responsibilities, potentially leading to higher job satisfaction and productivity. Employee wellness, particularly mental health, is directly linked to SDG 3, which aims to ensure healthy lives and promote well-being at all ages.

7 | Conclusion

This study aimed to explore the apparent discrepancies between defined security policies and their actual implementation within roles and responsibilities in the Swedish defense sector, focusing on a highly regulated and sensitive industry where adherence to security standards is not just expected but crucial. The aim was to uncover the realities behind formalized security protocols and the actual daily practices that influence these roles. Through a detailed case study approach, this research has identified significant gaps between the theoretical frameworks of security policies and their practical applications, particularly within role management and responsibility assignments.

During the investigation, it was notably apparent that only a select group of employees involved in specific processes within the company's software supply chain management had formalized roles and responsibilities. This selective formalization of roles within such a critical sector as software supply chain management raises serious concerns about the organization's comprehensive implementation of Information Security Management System (ISMS) protocols. The standards, particularly ISO/IEC 27001, are intended to ensure clear role definitions across all levels and sectors of the organization, yet this seems not to be fully realized. This discovery raises critical concerns about the implementation and efficacy of ISMS protocols, which theoretically require clear definitions of roles and responsibilities across all levels and sectors of the organization. The lack of formally defined roles not only undermines the integrity of the organization's security management, but also, as shown in the results, can significantly impact operational efficiency and risk management. Employees without clear roles have described a struggle to understand their specific duties and responsibilities, leading to potential security lapses, inefficiencies, and decreased job satisfaction. Thematic analysis revealed several discrepancies that underscore the challenges in aligning security policies with their execution.

The first research question (**Q1**) aimed to discover the discrepancies between defined security policies and their actual implementation in terms of roles and responsibilities. The analysis revealed that formal role descriptions often do not reflect actual tasks and responsibilities, leading to significant gaps between policy and practice. This undermines the effectiveness of security measures, as employees are left to interpret roles that do not align with their daily activities. There is also a significant lack of clear definitions and boundaries in roles, creating confusion and inefficiency, which opposes the organized method anticipated by the security policies. In addition, roles and responsibilities are frequently communicated informally and through direct interactions, rather than being clearly documented and standardized according to security protocols. The need for adaptability in roles also highlights a deviation from the rigid definitions typically outlined in security policies, indicating that flexibility is required but not well managed or supported. Furthermore, a significant finding was the distinct impact of these discrepancies on junior employees. Juniors often struggle with the lack of clear role definitions, feeling left to navigate their responsibilities without sufficient guidance. This contrasts sharply with senior employees, who, due to their experience and familiarity with the organizational culture, are less affected by the ambiguities of role definitions. The disparity in how role clarity affects employees differently based on their experience levels underscores the critical need for customized communication and role definition strategies within organizations.

The second question (**Q2**) explored the underlying reasons for these gaps. The analysis identified several key factors that contribute to these discrepancies. The overly formal nature of role descriptions makes them difficult to apply in practical, real-world scenarios, resulting in documents that do not translate into actionable guidance for employees. The informal means of communicating roles and relying on managerial discretion leads to inconsistencies in how roles are understood and implemented. Quick changes and growth within teams without corresponding updates to role definitions contribute to the misalign-

ment between policy and practice. Moreover, the use of tools like Workday primarily for classification rather than actual role management reflects a cultural and procedural gap in how roles are defined and maintained.

The findings of this study reveal significant discrepancies between the theoretical frameworks of security policies and their practical applications in terms of role management and responsibility assignments. These gaps extend beyond the defense sector, affecting any industry where the adherence to security standards is paramount. The central focus of the study was the exploration of roles and responsibilities within organizations. The findings reveal how formalized role descriptions often fail to reflect the actual roles and responsibilities that employees assume, leading to confusion and inefficiency. The lack of clear definitions and boundaries in the roles intensifies this problem, leaving employees to interpret their duties without sufficient guidance. In addition, the study highlights the impact of these discrepancies on different levels of employees. Junior employee members often struggle the most to navigate their responsibilities without clear guidance, while senior employee, with their experience, may adapt more easily to ambiguities. These findings underscore the universal challenge organizations face in effectively managing roles and responsibilities to ensure the smooth implementation of security protocols. By addressing these gaps and implementing strategies for clearer communication and role definition, organizations in various sectors can enhance their security measures and effectively mitigate potential risks.

7.1 Future work

This study has provided valuable information on the discrepancies between formal policies and their practical implementation regarding roles and responsibilities within an organization, specifically within the context of a defense company's software supply chain. These findings highlight significant gaps that could impact the overall security posture of the organization. Recognizing the limitations posed by the focus of the study on a single organization in a highly regulated sector using qualitative methods, future research could take several directions to expand and deepen these findings.

To overcome the limitations related to remote interviewing through Skype, future research should consider incorporating face-to-face interviews where feasible. This adjustment aims to capture non-verbal cues more effectively and achieve a deeper level of interaction, thus addressing the potential loss of rich communicative context in remote settings. Furthermore, by expanding the pool of participants beyond purposive sampling, future studies can improve the generalizability of the findings. Including a more diverse array of participants from different levels within the organization or even from similar organizations within the industry would validate the findings in a broader demographic and uncover additional insights that the initial study may have missed due to its narrow sample base. The limited sample size of ten interviews, while providing depth, may not capture all viewpoints within a large organization. To address this, future work could involve conducting a larger number of interviews or incorporating other data collection methods, such as surveys or focus groups. This expansion would ensure a more comprehensive coverage of employee experiences and opinions, addressing the representational limitations of the current study.

The subjectivity in qualitative analysis is also critical. Future studies might take a mixed-methods approach, combining qualitative findings with quantitative data. This technique would provide a more balanced perspective and reduce the impact of individual researcher bias, improve the overall validity and reliability of the findings, and address the inherent subjectivity in existing thematic analysis. Given the need to maintain company anonymity, which limits the detail that can be shared about specific organizational practices, future studies might explore similar contexts where more detailed disclosure is permissible. Alternatively, developing methods for discussing sensitive information in a way that maintains confidentiality but allows for a deeper exploration of context-specific dynamics would be beneficial. This approach addresses current limitations around the depth and specificity of the data. Furthermore, the flexibility allowed in the selection of the language for interviews, while accommodating the comfort of the participants, could affect the consistency of the interpretation of the data. Future studies should consider standardizing the interview language or employing professional translation services to ensure that linguistic variations do not influence the analysis. This change would address the limitation of the current study in terms of the variability in data interpretation caused by language differences.

Expanding the investigation to include different sectors such as healthcare or finance, where information security management is critically important, would not only validate the findings of this study, but also potentially broaden their applicability. Examining the link between policy-practice discrepancies and security breaches or compliance failures in these sectors could provide crucial insight to improve information security strategies. In addition, employing longitudinal studies would provide a dynamic view of how security policies and their interpretation evolve over time. This methodological approach would allow researchers to track the long-term effects of policy adjustments and continuous adaptations necessary to address emerging security threats, thus providing a temporal dimension that the current study lacks.

By addressing these specific limitations and areas for improvement in future studies, researchers can build on the foundational insights provided by this study. This comprehensive approach will significantly contribute to the development of more robust security frameworks that are theoretically sound and practically executable, thus enhancing the overall security resilience of organizations.

Bibliography

Alaskar, M., Vodanovich, S. and Shen, K. N. (2015), Evolvement of information security research on employees' behavior: A systematic review and future direction, *in* '2015 48th Hawaii International Conference on System Sciences', pp. 4241–4250.

Alkhadra, R., Abuzaid, J., AlShammari, M. and Mohammad, N. (2021), Solar winds hack: in-depth analysis and countermeasures, *in* '2021 12th International Conference on Computing Communication and Networking Technologies', pp. 1–7.

Amorosa, K. and Yankson, B. (2023), 'Human error - a critical contributing factor to the rise in data breaches: a case study of higher education', *Holistica Journal of Business and Public Administration* **14**(1), 110–132.

Andress, J. and Leary, M. (2017), Chapter 4 - why information security policies?, *in* J. Andress and M. Leary, eds, 'Building a Practical Information Security Program', Syngress, pp. 63–75.

Ashenden, D. (2008), 'Information security management: A human challenge?', *Information Security Technical Report* **13**(4), 195–201.

Braun, V. and Clarke, V. (2006), 'Using thematic analysis in psychology', *Qualitative Research in Psychology* **3**(2), 77–101.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), 'Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness', *MIS Quarterly* **34**(3), 523–548.

Caldwell, T. (2012), 'Training – the weakest link', *Computer Fraud & Security* **2012**(9), 8–14.

Choi, S., Martins, J. T. and Bernik, I. (2018), 'Information security: Listening to the perspective of organisational insiders', *Journal of Information Science* (016555151774828).

Costantino, G., Marra, A. L., Martinelli, F. and Matteucci, I. (2018), Candy: A social engineering attack to leak information from infotainment system, *in* '2018 IEEE 87th Vehicular Technology Conference (VTC Spring)'.

Culot, G., Nassimbeni, G., Podrecca, M. and Sartor, M. (2021), 'The iso/iec 27001 information security management standard: Literature review and theory-based research agenda', *The TQM Journal* **33**(7), 76–105.

Etikan, I., Musa, S. A. and Alkassim, R. S. (2015), 'Comparison of convenience sampling and purposive sampling', *American Journal of Theoretical and Applied Statistics* **5**(1), 1–4.

Gehem, M., Usanov, A., Frinking, E. and Rademaker, M. (2015), Front matter, *in* 'Assessing Cyber Security: A Meta-Analysis of Threats, Trends, and Responses to Cyber attacks', Hague Centre for Strategic Studies, pp. 2–4. http://www.jstor.org/stable/resrep12567.1.

Gerring, J. (2004), 'What is a case study and what is it good for?', *The American Political Science Review* **98**(2), 341–354. http://www.jstor.org/stable/4145316.

Golafshani, N. (2003), 'Understanding reliability and validity in qualitative research', *The Qualitative Report* **8**(4), 597–606.

Hammarberg, K., Kirkman, M. and de Lacey, S. (2016), 'Qualitative research methods: When to use them and how to judge them', *Human Reproduction* **31**(3), 498–501.

Hancock, J. and Tessian (2022), 'Psychology of human error 2022', Tessian. https://www.tessian.com/resources/psychology-of-human-error-2022/.

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K. and Stantchev, V. (2022), 'A process framework for information security management', *International Journal of Information Systems and Project Management* .

Hennink, M. and Kaiser, B. N. (2022), 'Sample sizes for saturation in qualitative research: A systematic review of empirical tests', *Social Science & Medicine* **292**, 114523.

Höne, K. and Eloff, J. H. P. (2002), 'Information security policy—what do international information security standards say?', *Computers & Security* **21**(5), 402–409.

IBM (2023), 'Cost of a data breach report 2023'. https://www.ibm.com.

Inuwa, M. (2017), 'Relationship between job equity and performance of employee: A literature review', *International Journal of Business and Management Future* **1**, 14–21.

ISO/IEC, 27001 (2022), 'Iso/iec 27001:2022 information security, cybersecurity and privacy protection — information security management systems — requirements'. ISO.

Kadam, A. W. (2007), 'Information security policy development and implementation', *Information Systems Security* **16**, 246 – 256.

Kyngäs, H., Mikkonen, K. and Kääriäinen, M., eds (2020), *The application of content analysis in nursing science research*, 1 edn, Springer Cham.

Lowry, P. B. and Moody, G. D. (2014), 'Proposing the control-reactance compliance model (crcm) to explain opposing motivations to comply with organisational information security policies', *Information Systems Journal* **25**(5), 433–463.

Lundgren, M. and Bergström, E. (2019), 'Dynamic interplay in the information security risk management process', *International Journal of Risk Assessment and Management* **22**(2), 212.

Mack, N., Woodsong, C., Macqueen, K., Guest, G. and Namey, E. (2005), *Qualitative research methods: A data collector's field guide*, Family Health International.

Makwana, D., Engineer, P., Dabhi, A. and Chudasama, H. (2023), 'Sampling methods in research: A review', *International Journal of Trend in Scientific Research and Development (IJTSRD)* **7**(3), 762–768. https://www.ijtsrd.com/papers/ijtsrd57470.pdf.

Malatji, M. (2023), Management of enterprise cyber security: A review of iso/iec 27001:2022, *in* '2023 International Conference On Cyber Management And Engineering (CyMaEn)', pp. 117–122.

Mathers, N., Fox, N. and Hunn, A. (1998), *Trent Focus for Research and Development in Primary Health Care: Using Interviews in a Research Project*, Trent Focus.

MSB (2015), 'Vad är informationssäkerhet?'. https://www.informationssakerhet.se.

Nieles, M., Dempsey, K. and Pillitteri, V. Y. (2017), *An introduction to information security.*

Niemimaa, E. (2016), A practice lens for understanding the organizational and social challenges of information security management, *in* 'PACIS 2016 Proceedings', p. 58. http://aisel.aisnet.org/pacis2016/58.

Niemimaa, E. and Niemimaa, M. (2017), 'Information systems security policy implementation in practice: From best practices to situated practices', *European Journal of Information Systems* **26**(1), 1–20.

Nikander, J., Manninen, O. and Laajalahti, M. (2020), 'Requirements for cybersecurity in agricultural communication networks', *Computers and Electronics in Agriculture* **179**, 105776.

NIST (2024), The nist cybersecurity framework (csf) 2.0, NIST Cybersecurity White Paper NIST CSWP 29, National Institute of Standards and Technology, Gaithersburg, MD.

Njenga, K. and Brown, I. (2012), 'Conceptualising improvisation in information systems security', *European Journal of Information Systems* **21**(6), 592–607.

Nordlund, P. (2022), 'Sweden and swedish defence – introduction to the special issue', *Defence and Peace Economics* **33**(4), 387–398.

Peltier, T. R., Peltier, J. and Blackley, J. A. (2003), 'Information security fundamentals'.

Photopoulos, C. (2008), Chapter 4 - data security policy, *in* C. Photopoulos, ed., 'Managing Catastrophic Loss of Sensitive Data', Syngress, pp. 93–124.

PwC (2015), 'Information security breaches survey'. https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf.

Rohan, R., Papasratorn, B., Chutimaskul, W., Hautamäki, J., Funilkul, S. and Pal, D. (2023), Enhancing cybersecurity resilience: A comprehensive analysis of human factors and security practices aligned with the nist cybersecurity framework, Association for Computing Machinery.

Sayed, Z., Bandukwala, D., Idrisi, A., Faki, A., Shaikh, E. A., Shaikh, S. and Mirza, N. B. (2023), 'A guide to become nist compliant', *International Journal of Advanced Research in Science, Communication and Technology* .

Singh, A. N. and Gupta, M. (2017), 'Information security management practices: Case studies from india', *Global Business Review* **20**(1), 253–271.

Singh, A. N., Gupta, M. P. and Ojha, A. (2014), 'Identifying factors of "organizational information security management"', *Journal of Enterprise Information Management* **27**(5), 644–667.

Siponen, M. (2006), 'Information security standards focus on the existence of process, not its content', *Communications of the ACM* **49**(8), 97.

Siponen, M. and Willison, R. (2009), 'Information security management standards: Problems and solutions', *Information & Management* **46**(5), 267–270.

Solms, R. V. and van Niekerk, J. (2013), 'From information security to cyber security', *Computers & Security* **38**, 97–102.

Soomro, Z. A., Shah, M. H. and Ahmed, J. (2016), 'Information security management needs more holistic approach: A literature review', *International Journal of Information Management* **36**(2), 215–225.

Steckler, A., McLeroy, K. R., Goodman, R. M., Bird, S. T. and McCormick, L. (1992), 'Toward integrating qualitative and quantitative methods: An introduction', *Health Education Quarterly* **19**(1), 1–8.

Stewart, H. and Jürjens, J. (2017), 'Information security management and the human aspect in organizations', *Information and Computer Security* **25**(5), 494–534.

Suorsa, M. and Helo, P. (2024), 'Information security failures identified and measured – iso/iec 27001:2013 controls ranked based on gdpr penalty case analysis', *Information Security Journal: A Global Perspective* **33**(3), 285–306.

Taherdoost, H. (2022), 'Cybersecurity vs. information security', *Procedia Computer Science* **215**, 483–487.

Theofanidis, D. and Fountouki, A. (2019), 'Limitations and delimitations in the research process', *Perioperative Nursing (GORNA)* **7**(3), 155–162.

Timmermans, J. (2022), Exploring the multifaceted relationship of compliance and integrity—the case of the defence industry, *in* R. Beeres, R. Bertrand, J. Klomp, J. Timmermans and J. Voetelink, eds, 'NL ARMS Netherlands Annual Review of Military Studies 2021', NL ARMS. T.M.C. Asser Press, The Hague, pp. 93–113.

United Nations (2024), 'United nations sustainable development goals'. https://www.un.org/sustainabledevelopment/.

Welch, C. and Piekkari, R. (2006), 'Crossing language boundaries: Qualitative interviewing in international business', *MIR: Management International Review* **46**(4), 417–437. http://www.jstor.org/stable/40836096.

World Economic Forum (2022), 'The global risks report 2022'. https://www3.weforum.org.

Zammani, M. and Razali, R. (2016), 'An empirical study of information security management success factors', *International Journal on Advanced Science, Engineering and Information Technology* **6**, 904–913.

A | Interview Guide in Swedish

Introduktion

Hej och välkommen [deltagarnamn]! Tack för att du deltar i denna intervju. Mitt namn är Tara Alndawi och jag studerar för närvarande till en masterexamen i informatik med inriktning på integritet, information och cybersäkerhet vid Högskolan i Skövde. Den här intervjun är en del av min avhandling, där målet är att utforska skillnaderna mellan etablerade säkerhetspolicyer och deras praktiska genomförande i organisationer, speciellt när det gäller roller och ansvarsområden. Huvudsyftet med studien är att identifiera eventuella skillnader mellan dokumenterade säkerhetsprotokoll och deras tillämpning i verkligheten. Innan vi går vidare till intervjufrågorna vill jag informera dig om att ditt deltagande idag är helt frivilligt och att du när som helst kan välja att avbryta studien. All information du delar med oss idag kommer att hållas konfidentiell och resultaten presenteras anonymt. Vi har strikt följt din organisations regler för datalagring för att upprätthålla säkerhetsstandarderna. Låt mig veta om du har några frågor om ditt deltagande, hur dina data kommer att användas, eller om du har några andra funderingar. Innan vi börjar med intervjufrågorna, har du några tankar eller frågor?

Intervjufrågor

Q1: Beskriv din nuvarande roll, vad är dina huvudansvar?

Q2: Hur förklarades eller delegerades dessa ansvarsområden till dig?

Q3: Hur jämför det du faktiskt gör dagligen med den formella beskrivningen av din roll?

Q4: Kan du beskriva en situation där det fanns en skillnad mellan din formella rollbeskrivning och dina faktiska arbetsuppgifter?

Q5: Hur kommuniceras roller och ansvarsområden inom ditt team/avdelning?

Q6: Har du någonsin varit osäker på vad dina ansvarsområden var i en specifik situation? Vad hände?

Q7: Vilken påverkan har tydliga eller otydliga rollbeskrivningar på ditt arbete?

Q8: Vilka utmaningar har du mött på grund av otydliga roller eller ansvarsområden?

Q9: Hur har din roll och ansvarsområden utvecklats sedan du började här? Hur har du anpassat dig till dessa förändringar?

Q10: Vilket stöd finner du mest hjälpsamt när du tar på dig nya ansvarsområden eller roller eller när du känner dig förvirrad över dina ansvarsområden?

Q11: Vilka verktyg eller system använder du för att förstå och hantera dina ansvarsområden? Hur effektiva är de?

Q12: På vilka sätt skulle nuvarande verktyg eller plattformar kunna förbättras för att bättre stödja dig i din roll?

Avslutning

Sluttankar: Finns det något annat du skulle vilja tillägga som vi inte har täckt, särskilt när det gäller rolltydlighet eller arbetsansvar?

Tack: Din tid och insikter idag är mycket uppskattade. Tack för ditt engagemang, som kommer att ha en betydande inverkan på vår studie. Jag kommer att skicka en kopia av intervjuutskriften till dig som en del av vårt åtagande att vara noggranna och öppna. Detta ger dig möjlighet att granska vår diskussion och komma med eventuella tillägg eller klargöranden. Vi måste säkerställa att dina perspektiv och upplevelser är korrekt representerade i vår studie i detta steg.

B | Appendix: Interview Guide in English

Introduction

Hello and greetings [participant name]! Thank you for participating in this interview my name is Tara Alndawi and I am currently pursuing a Master's Degree in Informatics with a specialization in Privacy, Information, and Cybersecurity at Skövde University. This interview is part of my thesis research, which aims to explore the discrepancies between established security policies and their practical implementation within organizations concerning roles and responsibilities. The main objective of this study is to identify any disparities between the documented security protocols and their real world application. Before we get into the interview questions, i want to inform you that your participation today is entirely voluntary and you are free to withdraw from the study at any time. Any information you share today will be kept confidential with results presented anonymously. We have strictly adhered to your company's data storage regulations to maintain security standards. Please let me know if you have any questions about your participation, how your data will be used, and any concerns. Before we proceed with the interview questions, do you have any thoughts?

Interview Questions

Q1: Describe your current role, what is your primary responsibilities?

Q2: How were these responsibilities explained/delegated to you?

Q3: How does what you actually do on a daily basis compare with the formal description of your role?

Q4: Can you describe a situation where there was a difference between your formal role description and your actual work tasks?

Q5: How are roles and responsibilities communicated within your team/department?

Q6: Have you ever found yourself unsure about what your responsibilities were in a specific situation? What happened?

Q7: What impact does having clear or unclear role descriptions have on your work?

Q8: What challenges have you faced due to unclear roles or responsibilities?

Q9: How have your role and responsibilities evolved since you started here? How have you adapted to these changes?

Q10: What support do you find most helpful when taking on new responsibilities or roles or when feeling confused about your responsibilities?

Q11: What tools or systems do you use to understand and manage your responsibilities? How effective are they?

Q12: In what ways could current tools or platforms be improved to better support you in your role?

Conclusion

Final Thoughts: Is there anything else you would like to add that we have not covered, especially regarding role clarity or job responsibilities?

Thank You: Your time and insights today are highly appreciated. Thank you for your commitment, which will have a significant impact on our study. I will send you a copy of the interview print as part of our commitment to be careful and transparent. This gives you the opportunity to review our discussion and come up with any additions or clarifications. We need to ensure that your perspectives and experiences are correctly represented in our study at this stage.