CHALMERS
UNIVERSITY OF TECHNOLOGY

A Gap Analysis of Supply Chain Security Against ISO 28000 at a Defense Industry Company

A Case Study of Governance, Formalisation and Alignment

Master's thesis in The Supply Chain Management Master's Program

HILDA MALMFORS
TEODOR EDHAGE

DEPARTMENT OF TECHNOLOGY MANAGEMENT AND ECONOMICS

DIVISION OF SUPPLY AND OPERATIONS MANAGEMENT
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2026
www.chalmers.se

A Gap Analysis of Supply Chain Security Against ISO 28000 at a Defence Industry Company

A Case Study of Governance, Formalisation and Alignment

HILDA MALMFORS
TEODOR EDHAGE

Department of Technology Management and Economics
Division of Supply and Operations Management
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2026

A Gap Analysis of Supply Chain Security Against ISO 28000 at a Defense Industry Company
A Case Study of Governance, Formalisation and Alignment
HILDA MALMFORS
TEODOR EDHAGE

Supervisor: Gunnar Stefánsson, Supply and Operations Management
Examiner: Gunnar Stefánsson, Supply and Operations Management

Department of Technology Management and Economics
Chalmers University of Technology
SE-412 96 Gothenburg
Sweden
Telephone + 46 (0)31-772 1000

Gothenburg, Sweden 2026

A Gap Analysis of Supply Chain Security Against ISO 28000 at a Defence Industry Company
A Case Study of Governance, Formalisation and Alignment

HILDA MALMFORS
TEODOR EDHAGE

Department of Technology Management and Economics
Chalmers University of Technology

Abstract

Supply chain security has emerged as a strategically significant governance challenge for organisations operating in security sensitive industries. As hostile actors increasingly target supply chain dependencies to exploit vulnerabilities below the threshold of armed conflict, the need for structured and formalised governance of supply chain security has become a strategic imperative rather than a compliance obligation. This examination investigates the degree of alignment between existing supply chain security practices at an established defence and security industry organisation and the requirements of ISO 28000, with the aim of identifying areas of compliance, partial alignment and significant nonconformance across relevant organisational processes and supplier interfaces.

A mixed methods approach within a single case study framework is applied, combining semi-structured interviews with employees across relevant organisational functions and an analysis of internal company documentation. ISO 28000 serves as the analytical reference framework through which empirical material is systematically assessed.

The gap analysis reveals substantial alignment in several foundational areas where existing organisational structures and processes reflect the underlying governance logic of the standard. However, these structures are developed primarily in relation to ISO 27001 and are not configured to address supply chain security as a distinct governance domain. Partial alignment is identified across areas where relevant structures exist but fall short of the formalisation and institutional embeddedness required by the standard. Significant nonconformances are identified in the absence of formally designated compliance ownership, the reliance on informal coordination as a substitute for formal governance, the absence of measurable supply chain security objectives and the lack of a context analysis oriented towards the supply chain security environment.

The assessment concludes that the overall correspondence with ISO 28000 is partial rather than substantive. Supply chain security must be constituted as a governed domain in its own right, with formally designated compliance ownership, measurable objectives and structured verification mechanisms, before the organisation meaningfully pursues alignment with the standard.

Keywords: ISO 28000, Supply Chain Security, Gap Analysis, Security Governance & Management Systems

Acknowledgement

We would like to thank our supervisor and examiner, Gunnar Stefánsson, for his involvement in this thesis. We also wish to acknowledge our collaborating company for enabling the research and for contributing to the empirical foundation of the study. Finally, we express our appreciation to Chalmers University of Technology for providing the academic environment in which this thesis was developed.

Hilda Malmfors & Teodor Edhage
Gothenburg May 2026

Table of Contents

1. Introduction

The chapter introduces the background and frames the problem under investigation. It outlines how supply chains have become central to national security and explains why the studied organisation lacks a unified framework for supply chain security management. The purpose, research questions and delimitations of the study are presented.

1.1 Background

Supply chains form an essential part of modern societal organisation and national security, as they enable the continuous provision of goods, services and capabilities that sustain both civilian society and military operations. Swedish security authorities emphasise that many functions of importance for national security are no longer confined to traditional state or military structures. Instead, critical activities such as industrial production, logistics, energy supply, transportation systems and digital services are often carried out by civilian or private actors while simultaneously supporting the total defence. This development means that vulnerabilities within supply chains may have direct implications for national security even in situations characterised by heightened tension rather than open armed conflict (Försvarsmakten, 2025).

These structural dependencies must be understood in the context of an increasingly unstable security situation. The National Defence Radio Establishment (2024) and the Military Intelligence and Security Service (2025) assess that the current security situation is characterised by long term geopolitical confrontation. According to these assessments, hostile states increasingly employ a broad spectrum of measures that extend beyond conventional military force. Thus, cyber operations, sabotage, intelligence activities and influence operations are used to weaken adversaries, shape decision making and exploit vulnerabilities within societal systems while remaining below the threshold of armed conflict.

Within this context, supply chains constitute particularly attractive targets. The Military Intelligence and Security Service (2025) notes that hostile actors actively seek to identify weaknesses in critical flows, infrastructure and industrial capabilities that support both civilian society and military readiness. Interference with logistics, disruption of industrial production or manipulation of supply relationships may weaken national capability without requiring direct military confrontation. Given that supply chains frequently involve civilian entities with varying degrees of security awareness and protection, they may constitute vulnerable access points for intelligence collection or disruptive activities with potentially significant strategic effects. Furthermore, supply chains are exposed to a variety of disruptive factors, including natural disasters, armed conflict and terrorism, criminal activity and labour related disruptions. These

factors may interact and reinforce one another, meaning that even a single disruptive event may escalate rapidly and generate significant economic and societal effects at the national level (Thomas & Vaduva, 2015).

In addition to direct disruption, economic interdependence itself could increasingly function as a method of strategic influence. In a security environment characterised by intensified geopolitical rivalry, trade relations, financial infrastructures and supply dependencies could be leveraged to exert political pressure or constrain strategic choices. Supply chains are therefore not only vulnerable to sabotage or intelligence operations, but may also serve as instruments through which power is exercised below the threshold of armed conflict. Such dynamics blur the distinction between economic cooperation and strategic competition, reinforcing the security relevance of seemingly commercial relationships (World Economic Forum, 2026).

The Swedish Security Service (2025) further emphasises that these challenges are intensified by the expansion of the total defence system and Sweden's integration into Nato. As preparedness measures increase, a growing number of civilian organisations and private companies become involved in activities that are security sensitive. This expansion creates new interdependencies between civilian and military domains and increases the importance of understanding how vulnerabilities may arise outside traditional military structures.

At the same time, the evolving security environment has prompted increasing emphasis on resilience and strategic autonomy in critical sectors such as energy, food supply, digital infrastructure and industrial production. While complete self sufficiency is neither feasible nor economically desirable, diversification of supply relationships and reduction of excessive dependencies are increasingly framed as security imperatives rather than purely economic considerations. Efforts to strengthen domestic capacity, broaden supplier networks and enhance collective resilience reflect an emerging recognition that highly concentrated dependencies may generate strategic vulnerabilities (World Economic Forum, 2026).

The assessments of the Swedish Security Service (2025), the National Defence Radio Establishment (2024) and the Military Intelligence and Security Service (2025) illustrate that supply chains have become deeply embedded in the broader security environment. Their vulnerabilities are shaped not only by the risk of direct disruption, but also by the strategic use of economic interdependence in an increasingly fragmented international system. These dynamics reflect the interaction between civilian and military interdependence, increasing technological reliance and a complex and evolving threat landscape characterised by hybrid methods, economic coercion and activities short of armed conflict. An understanding of this security environment is necessary to explain the emergence of supply chain security challenges and their growing prominence in current security discussions.

In response to the evolving threat landscape and the growing recognition of supply chain vulnerabilities as strategic risks, organisations operating in security sensitive sectors have increasingly directed attention towards structured governance frameworks capable of providing systematic and auditable approaches to supply chain security management. The development of formalised management systems has emerged as a central mechanism through which organisations seek to strengthen supply chain resilience, establish consistent security practices across supplier networks and demonstrate accountability to customers, regulators and alliance partners. Within this context, a number of internationally recognised frameworks and standards have established themselves as central reference points for the structured and risk based governance of supply chain security. These include management system standards such as ISO 28000 (ISO, 2022). Organisations increasingly regard such frameworks not as isolated instruments of compliance, but as complementary governance references that, taken together, provide a broader foundation for addressing the multidimensional risk environment inherent to modern supply chains.

1.2 Problem Description

Customers are increasingly requesting evidence that the organisation, an established actor within the defence and security industry, operates in accordance with the ISO 28000 supply chain security management system. The standard is also relevant from an internal organisational perspective, as it addresses the protection of business critical assets such as information, research and development activities, intellectual property rights, employees and brand value. A systematic approach to supply chain security is therefore closely linked to the organisation's long term competitiveness, organisational resilience and ability to support continued growth, profitability and shareholder value.

For organisations that are not certified according to ISO 28000, or that have not yet established a uniform organisational framework for interpreting and managing the requirements of the standard, it may be challenging to obtain a clear overview of how supply chain security is governed across the organisation. In such contexts, existing documents, procedures and processes may correspond to selected elements of ISO 28000, while not necessarily being structured within a common framework that clarifies how the requirements are understood, implemented and followed up in practice.

A lack of a shared organisational reference framework may make it difficult to assess overall alignment with ISO 28000 and to identify areas where further development could be needed. It may also create challenges in coordinating supply chain security related responsibilities across organisational functions, particularly where processes, priorities and interpretations of security requirements vary. A clearer organisational approach to how ISO 28000 requirements could be interpreted and implemented may therefore support more coordinated and systematic management of supply chain security. This could strengthen internal alignment, support the protection of critical

assets and provide a clearer basis for integrating security considerations into organisational processes, while also enabling a more transparent demonstration of supply chain security management in relation to the expectations of external stakeholders.

1.3 Purpose and Research Questions

The purpose is to examine and evaluate the current state of supply chain security within an established actor in the defence and security industry, with particular consideration given to the characteristics and challenges associated with supply chains operating under high security requirements. Although the organisation is not currently certified in accordance with ISO 28000, existing supply chain security practices within the upstream supply chain are described as being aligned with the principles of the standard. However, the extent to which these practices correspond to the specific requirements of ISO 28000 has not previously been systematically assessed.

To address this, ISO 28000 is used as an analytical reference framework and a structured gap analysis is conducted to assess existing supply chain security practices across relevant organisational processes and functions. The analysis aims to identify areas of compliance, as well as discrepancies and limitations, in order to develop an understanding of the organisation’s current level of supply chain security maturity. In addition, the study aims to establish a structured foundation for how supply chain security management could be organised and developed in alignment with ISO 28000, thereby contributing to a more strategic and systematic approach to supply chain security within the organisation. The findings are intended to support informed decision making and future initiatives to strengthen and formalise supply chain security management, as well as clarify what would be required to achieve ISO 28000 certification.

Three research questions guide the analysis. The first concerns the governance implications of the standard itself and examines how implementing ISO 28000 would influence the organisation's supply chain security related practices. The second question addresses how current organisational practices correspond to the requirements of ISO 28000. The third moves to a more specific level of assessment, identifying gaps between existing practices and ISO 28000 requirements across relevant organisational processes and supplier interfaces. When considered together, these three questions provide a structured progression from the theoretical implications of the standard to an assessment of overall alignment and a detailed identification of areas requiring development.

RQ1:
How would an implementation of ISO 28000 influence supply chain security related practices within the organisation?

RQ2:
How do current organisational practices correspond to the requirements of ISO 28000?

RQ3:
What gaps can be identified between existing practices and the requirements of ISO 28000 across relevant organisational processes and supplier interfaces?

1.3.1 Objectives

The objective is to conduct a structured and systematic assessment of supply chain security management within the organisation by analysing existing practices in relation to the requirements of the ISO 28000 standard. The assessment aims to establish a documented and comprehensive overview of how supply chain security is currently addressed across relevant organisational processes and functions, as well as to determine the degree of alignment with the standard. Furthermore, the objective is to identify key strengths, gaps and areas requiring further development. The results are intended to provide an analytically grounded basis for informed decision making regarding the standardisation and formalisation of supply chain security management within the organisation, as well as to support the potential development of an ISO 28000 aligned supply chain security management system.

1.4 Limitations

The scope and level of detail of the analysis are influenced by several limitations. The analysis focuses primarily on organisational structures and processes related to supply chain security management within the company's group level functions rather than examining all organisational functions across the company. Consequently, the analysis reflects the perspective and responsibilities of group level and may therefore not fully capture variations in practices across different parts of the organisation.

Although the analysis is conducted within group level functions, input from representatives of other functional areas has been incorporated in order to capture perspectives from different parts of the organisation. This approach supports the development of a broader understanding of existing practices. However, it does not constitute a comprehensive assessment of all business units and differences in processes, priorities and interpretations of security related responsibilities across organisational functions may therefore not be fully reflected in the analysis. The purpose is to establish a structural foundation for supply chain security management aligned with ISO 28000. Accordingly, the analysis focuses primarily on organisational

governance, processes and management practices rather than detailed operational implementation across all parts of the organisation.

The scope of the analysis is also influenced by considerations related to confidentiality and information sensitivity. Access to data and the level of detail presented in the analysis are therefore dependent on what information could be shared and documented in accordance with the company's internal guidelines. It should also be noted that the analysis does not constitute a formal certification audit against ISO 28000. Instead, the standard is used as an analytical reference framework to structure the assessment of existing practices and identify potential areas for improvement.

2. Methodology

The chapter presents and justifies the methodological choices made. It describes the mixed methods approach within a single case study design, explains how data were collected through semi structured interviews and internal documentation as well as outlines the construction of the gap analysis instrument. Considerations of validity, reliability and the handling of confidential material are also addressed.

2.1 Research Design and Strategy

To address the research questions, a mixed methods approach is applied, combining qualitative and quantitative elements within a single case study design. This methodological choice reflects the dual purpose of the investigation of examining how supply chain security is currently organised and practised in relation to the requirements of ISO 28000, while also conducting a structured gap analysis that produces systematic assessments across defined organisational domains. The combination of qualitative and quantitative methods is considered appropriate when a research problem requires both an exploration of contextual meaning and a more structured evaluation of observable conditions (Creswell & Creswell, 2018). Thus, neither approach alone would adequately address the research questions, as qualitative data is necessary to understand how security responsibilities and processes are interpreted and enacted in practice, while the gap analysis requires a systematic, criteria based assessment of the extent of alignment with the standard.

The overarching design of the study is a single case study, with the organisation constituting the unit of analysis. This design is appropriate because it enables an examination of supply chain security practices within a practical organisational context, while also assessing its alignment with the requirements of ISO 28000. According to Yin (2018), a single case study is suitable when the case is particularly informative in relation to the research problem. The organisation is regarded as such a case, given its organisational scale, the complexity of its operations and the relevance of supply chain security to its broader operating environment. The design therefore supports the objectives of developing analytical depth and a thorough organisational understanding rather than broad statistical generalisation (Creswell & Creswell, 2018).

The qualitative component of the investigation comprises semi structured interviews with respondents from various organisational functions and levels, as well as an analysis of internal organisational documentation. These data sources enable an examination of how supply chain security responsibilities and processes are formally defined and how they are understood and applied in practice. The qualitative dimension is essential for capturing the contextual, interpretive and organisational dimensions of supply chain security governance that cannot be reduced to standardised criteria alone (Bryman, 2016). The quantitative component is operationalised through a structured

gap analysis, in which existing organisational practices are systematically assessed against the specific clause requirements of ISO 28000. This assessment provides a structured overview of the degree of alignment across defined organisational domains, enabling the identification of both areas of compliance and areas requiring further development. The integration of these two methodological components enables the analysis to address the research questions in a coherent and comprehensive manner, combining interpretive richness with analytical structure (Creswell & Creswell, 2018). The overall research process is illustrated in Figure 1. The figure presents how the literature review and theoretical framework inform the collection of empirical data and the construction of the gap analysis instrument and how these two elements then come together to produce the gap analysis findings.

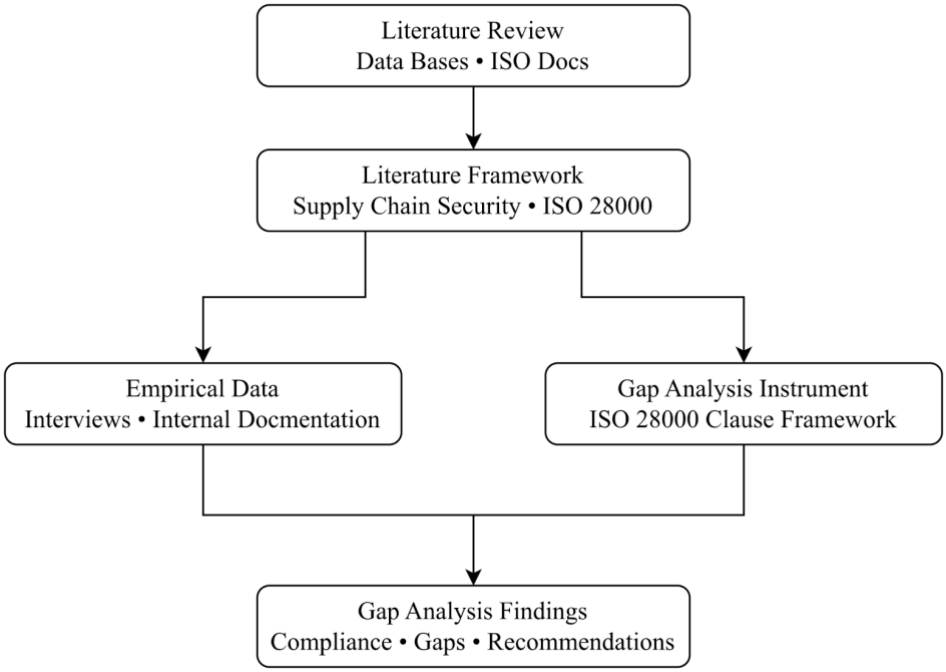

Figure 1. Research Process Overview.

Given the use of multiple methods and data sources in relation to three distinct research questions, it is necessary to specify how each question is addressed methodologically. Figure 2 therefore illustrates the primary relationship between each research question and its corresponding methods and data sources. It indicates that RQ1 is addressed primarily through the literature review, though also informed by insights emerging from the semi-structured interviews and that RQ2 draws additionally on the interviews and internal documents. RQ3 then synthesises these empirical sources through the gap analysis. While this suggests a certain sequential logic, in practice the methods overlap and inform one another iteratively throughout the research process. Considered together, the two figures provide a comprehensive methodological overview, with Figure 1 presenting the overall logic and sequence of the research process and Figure 2 demonstrating how the individual research questions are operationalised within that framework.

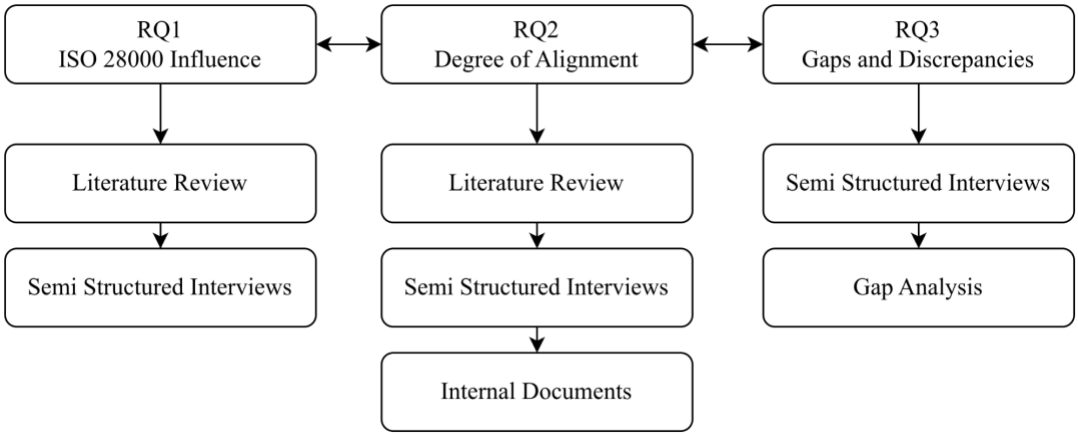

Figure 2. Research Questions and The Primary Corresponding Methods.

2.2 Data Collection

The empirical data comprises both primary and secondary sources. The use of multiple data sources is considered appropriate in qualitative and mixed methods research, as it enables a broader and more informed understanding of the organisational processes and practices under investigation (Bryman, 2016). Primary data were collected through semi structured interviews with employees across different organisational functions and hierarchical levels, whose roles were connected in various ways to supply chain security, procurement, risk management and internal governance. Secondary data consisted of internal company documentation related to supply chain security and associated areas, including materials describing relevant processes, responsibilities and organisational structures. The combination of interview data and internal documentation enabled an examination of both how relevant practices and responsibilities were described by employees and how these were formally expressed in documented structures and governance arrangements. The selection of both primary and secondary sources was guided by the requirements of ISO 28000, as well as by the company's established global management system and security management system.

2.2.1 Literature Review

The literature review serves to establish the theoretical and conceptual foundation of the investigation, to contextualise the research within existing knowledge and to support the analytical framework applied in the gap analysis. Thomas (2021) asserts that a literature review constitutes an essential component of any research endeavour, including case studies, as it provides the conceptual basis from which the object of investigation is approached and understood. Yin (2018) similarly emphasises that prior theoretical knowledge should inform both the design of the case study and the interpretation of empirical findings, thus ensuring that the investigation is firmly grounded in existing research.

The literature review takes a thematic and structured approach, combining systematic search procedures with the thematic organisation of the material collected. Rather than treating the literature as an undifferentiated body of knowledge, the review is organised around thematic areas that together constitute the theoretical framework. These are supply chain security, security governance in complex supply chains, risk management in upstream supply chains, management systems and organisational formalisation as well as ISO 28000 as an operational framework. This thematic structure ensures that each dimension of the research problem is adequately grounded in relevant theory and prior research (Saunders et al., 2023).

The structured component is operationalised through an iterative search process, the principles of which are shown in Figure 3. An initial set of keywords was identified based on the research questions and the central concepts of each thematic area. These were used to search established academic databases, with filters applied for year of publication and document type. The results were then screened for relevance based on the title, abstract and content. Selected items were then entered into the review. This process was repeated for each thematic area, with the keyword combinations being refined based on the material identified in the preceding rounds. This continued until a sufficient and coherent set of literature had been compiled for each theme. In accordance with Thulesius (2021), the review was conducted with a deliberate effort to engage with the existing literature impartially, acknowledging that preconceptions regarding the subject of investigation could otherwise influence source selection and interpretation.

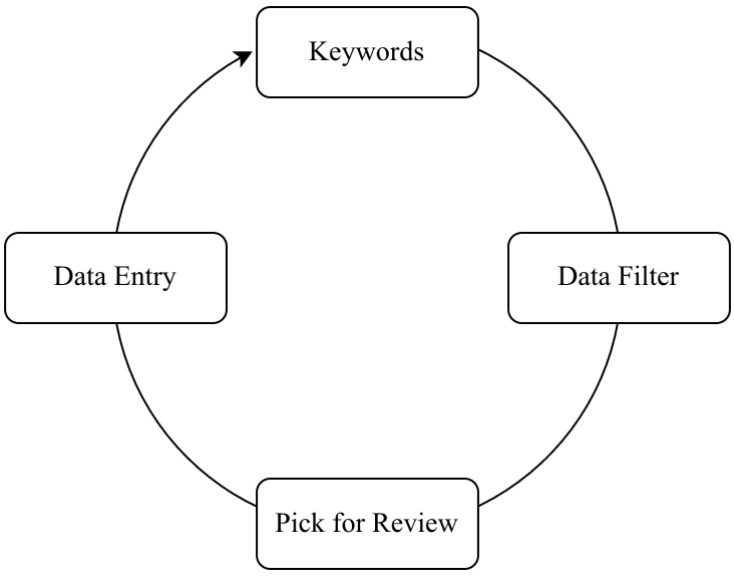

Figure 3. Iterative Literature Search Process.

2.2.2 Empirical Data

The empirical data consists of both primary and secondary sources. Qualitative research often draws on different types of empirical material to develop a broader understanding of the area investigated (Bryman, 2016). Flick (2009) also emphasises that the use of multiple qualitative data sources may contribute to a more nuanced understanding of social and organisational processes.

Primary data were collected through semi structured interviews with employees across different organisational functions and hierarchical levels, whose roles were linked in various ways to supply chain security, procurement, risk management and internal governance. Secondary data consisted of internal company documentation related to supply chain security, risk management and associated areas, including materials describing relevant processes, responsibilities and organisational structures. The selection of these documents was guided by the requirements of ISO 28000, as well as by the company's established global management system and security management system.

The combination of interview data and internal company material enabled an examination of both how relevant organisational practices, responsibilities and processes were described by employees and how these were formally expressed in documented structures and management arrangements. In line with Bryman (2016), the use of different forms of empirical material strengthened the basis for developing a broader understanding of the area investigated. Flick (2009) similarly highlights that combining qualitative sources could make it possible to offer a more comprehensive view of different dimensions of organisational processes and practices.

2.2.2.1 Primary Data from Interviews

The primary data consisted of semi structured interviews with employees representing different organisational functions and levels. The interviewees were involved in various aspects of supply chain security, procurement, risk management, internal governance and related organisational processes. Semi structured interviews were considered appropriate, as this format made it possible to address predefined themes while still allowing flexibility for respondents to elaborate on issues relevant to their specific roles and responsibilities. As Brinkmann and Kvale (2015) note, semi structured interviews are particularly suitable when the purpose is to explore participants' experiences and understandings while maintaining a certain degree of structure across interviews. Flick (2009) similarly argues that this interview format enables the combination of thematic guidance with openness to context specific insights.

The use of semi structured interviews made it possible to collect empirical material on how relevant organisational structures, responsibilities and processes were understood and described by individuals involved in different parts of the organisation. The interview format was particularly suitable because the respondents had different

professional backgrounds and areas of responsibility, which meant that the same broad themes needed to be approached from somewhat different perspectives. For this reason, the interview guides (see Appendix 1) were adapted to the specific responsibilities of each respondent, while maintaining a common thematic structure related to the purpose and the areas addressed in ISO 28000. This ensured a consistent basis for comparison between the interviews, while enabling respondents to elaborate on role specific practices and organisational conditions in line with the qualitative interviewing approach described by Brinkmann and Kvale (2015).

2.2.2.2 Selection of Interview Participants

The interview participants were selected through a purposive sampling strategy. Bryman (2016) describes purposive sampling as a strategy in which participants are selected on the basis of their relevance to the research questions and their expected ability to contribute knowledge of the subject under investigation. This approach was considered appropriate as the intention was not to ensure statistical representativeness, but rather to obtain informed perspectives from individuals with practical insight into the organisational processes relevant to the objectives. Thus, a total of 15 interviews were conducted.

The selection of participants was guided by the structure and requirements of ISO 28000, with the intention of identifying individuals whose roles were connected to organisational processes corresponding to different parts of the standard. The selection was also influenced by the company's established global management system and security management system, since these internal structures shaped how responsibilities and processes were organised in practice. In order to preserve confidentiality, the specific roles represented in the interview sample are not described in greater detail. In addition to the formal interviews, an ongoing dialogue was maintained with one respondent who served as the main contact person from the company side. This contact supported the practical conduct of the research by facilitating access to relevant functions, documents and organisational information and by clarifying aspects of the company's structures and processes when needed. This dialogue was not treated as a formal interview source, but as contextual and practical support during the research process.

The purposive selection of interviewees was intended to ensure that the empirical material reflected the perspectives of individuals in different organisational positions and functional areas, while remaining focused on roles considered relevant to the research purpose. As emphasised by Brinkmann and Kvale (2015), the strength of qualitative interviewing depends not on the number of respondents, but on the relevance and quality of the accounts provided by participants with experience of the subject under examination.

2.2.2.3 Secondary Data from Company Material

In addition to the primary data, the empirical material also included secondary data in the form of internal company material. This material consisted not only of formal documents, but also of other internally available material, including descriptions of processes, responsibilities, structures and management arrangements. These were used to provide a formal organisational perspective on the issues addressed in the interviews.

The inclusion of internal company material enabled an examination of how relevant organisational arrangements were formally described and structured within the organisation. In this regard, the material complemented the interview data by providing insight into how roles, responsibilities, working methods and governance arrangements were formally documented within the existing management systems. Boréus and Kohl (2018) explain that written material may be analysed systematically in order to identify how structures, meanings and formalised practices are expressed in text. In this regard, such material was particularly relevant, as the purpose was not only to understand how organisational practices were described by employees, but also how these practices were reflected in internal structures and formal arrangements.

The secondary material was examined in relation to the requirements of ISO 28000, as well as in relation to the company's established global management system and security management system. This made it possible to assess how relevant organisational processes and responsibilities were formally framed and their relevance to the areas addressed in the standard.

2.2.2.4 Selection of Secondary Material

The selection of secondary material was guided by its relevance to the broader objectives of the analysis and the organisational areas covered by ISO 28000. More specifically, material was included if it was considered relevant for understanding how processes, responsibilities and governance arrangements related to supply chain security were formally defined and managed within the company.

The selection was also informed by the company's established global management system and security management system, which provided an internal framework for identifying material of particular relevance. Thus, the selection was based on the material's relevance to organisational responsibilities, documented procedures, governance structures and process descriptions considered significant to the empirical analysis. This is consistent with Bryman's (2016) description of purposive selection, in which empirical material is selected on the basis of its relevance to the purpose and research questions of the investigation. The intention was not to include all available internal material, but rather to select material considered particularly relevant for understanding the formal organisational conditions surrounding the processes and responsibilities under examination.

2.2.2.5 Handling of Data and Confidentiality

The handling of the empirical material was guided by considerations of confidentiality and the sensitivity of the information involved. As the Swedish Research Council (2024) states, good research practice requires ethical reflection throughout the entire research process, from planning and data collection to analysis and publication. Thus, the interviews were not recorded or transcribed due to internal confidentiality considerations and the sensitivity of the topics discussed. Instead, detailed notes were taken during each interview and used as the basis for the analysis. This approach was considered appropriate given the organisational context and the information shared. Brinkmann and Kvale (2015) emphasise that interview research involves both practical and ethical judgement, making responsible handling of sensitive interview material particularly important. Bryman (2016) similarly identifies participant protection and careful handling of research material as central aspects of social research practice.

The interview notes were treated as confidential research material and were used only for the purposes of the analysis. The same applied to the internal company material used as secondary data, some of which contained sensitive information. In the presentation of the empirical material, care was taken not to disclose sensitive operational details or information that could identify specific internal vulnerabilities, individuals or confidential organisational arrangements.

2.3 Assessment of Methodology

The chosen methodological approach is tailored to the objectives of the investigation, which are to examine how supply chain security is organised and implemented in practice and to assess the extent to which existing practices correspond to the requirements of ISO 28000. A mixed methods design within a single case study framework is particularly suitable when the objective is to understand how formal structures are interpreted and applied in practice rather than to measure predefined variables in multiple settings (Yin, 2018). As Creswell and Creswell (2018) observes, case study research prioritises analytical depth within a specific context, which limits the extent to which the findings could be generalised beyond that setting.

2.3.1 Validity

Validity is addressed through the planning of data collection and analysis, focusing on how supply chain security is understood and implemented in different organisational settings. In qualitative and mixed methods research, validity is closely associated with the credibility of interpretations and the extent to which the findings reflect the investigated perspectives and practices (Bryman, 2016).

The empirical material comprises semi structured interviews with respondents from positions related to supply chain security, procurement and internal governance. Interview guides were adapted to different respondent groups while maintaining a

shared thematic structure, enabling the collection of both function specific contributions and broader organisational patterns to be collected. As Saunders et al. (2023) note, semi structured interviews are particularly appropriate for the exploration of organisational processes in different functional areas, as consistency and flexibility in data collection may be achieved. The interviews were conducted as open, dialogue oriented conversations in which predefined themes guided the discussion while allowing respondents to expand on their experiences and practices.

Since interviews were not recorded due to confidentiality considerations, detailed notes were taken during each session and expanded immediately afterwards. Although the absence of recordings limits the possibility of capturing exact wording, systematic documentation combined with the immediate expansion of notes supports the credibility of the findings by ensuring that the empirical material accurately reflects the content of each interview (Creswell & Creswell, 2018). Validity is further reinforced through the combination of multiple data sources. Interview data was analysed in relation to internal organisational documents and the ISO 28000 standard, enabling comparison between formalised structures and their understanding and application in practice. This analytical comparison supports the identification of consistencies and discrepancies between documented procedures and operational realities, thus reinforcing the interpretation of organisational processes (Bryman, 2016).

The ISO 28000 standard functions as a structured reference framework guiding the interpretation of empirical material. The analysis is anchored in a defined set of criteria by relating observed practices to the requirements of the standard, while remaining sensitive to the specific organisational context in which those requirements are applied. Given the scope and complexity of the organisation, the investigation does not intend to cover all possible perspectives related to supply chain security. Validity is instead strengthened by focusing on respondents with direct involvement in relevant processes, ensuring that the empirical material is grounded in practical experience and organisational understanding.

2.3.2 Reliability

Reliability in qualitative and mixed methods research concerns the consistency, transparency and traceability of the research process, rather than the ability to reproduce identical results across different settings. As Bryman (2016) argues, the emphasis is placed on how systematically data is generated and interpreted, while Creswell and Creswell (2018) highlights the importance of clearly documented procedures that enable others to understand how conclusions have been reached. Data collection was conducted using semi structured interview protocols adapted to different organisational roles. While interview guides varied depending on the respondent's function, a consistent set of themes guided all interviews, addressing similar areas, ensuring that comparable topics were covered while maintaining flexibility in how contributions were collected (Saunders et al., 2023). Empirical material was documented through

careful note taking during each session and expanded immediately afterwards, providing a consistent and traceable basis for the subsequent analysis.

The analytical process involved a structured and systematic procedure, with interview data examined in relation to the ISO 28000 standard as a common reference point. Applying the same analytical framework to all interviews ensured that comparable types of data were assessed using consistent criteria. Responses were compared both across respondents in similar roles and across different organisational functions, supporting a consistent analytical process. Variations in responses were addressed through systematic comparison rather than treated as inconsistencies, with differences analysed in relation to role specific perspectives and organisational context. Given the size and complexity of the organisation, the investigation relies on a purposive selection of respondents representing important functions within supply chain security and procurement. Reliability is supported through a transparent and structured research process, including consistent data collection procedures, systematic documentation and a clearly defined analytical framework guiding the interpretation of empirical material (Bryman, 2016).

2.4 Gap Analysis Methodology and Assessment Structure

The gap analysis is operationalised through a structured comparison between existing organisational practices and the clause requirements of ISO 28000. The purpose of the gap analysis is not to produce a formal certification audit but to systematically assess the degree to which current supply chain security practices correspond to the requirements of the standard, thereby identifying areas of alignment, partial compliance and significant nonconformance across defined organisational domains.

The analytical structure is organised around the clause framework of ISO 28000, which encompasses the organisational context, leadership, planning, support, operation, performance evaluation and improvement (ISO, 2022). Each clause was used as an evaluative reference point against which the empirical material was assessed. This approach is consistent with the use of ISO 28000 as an analytical reference framework rather than a prescriptive compliance checklist, ensuring that the assessment remains sensitive to the specific organisational context while maintaining a systematic and comparable basis for evaluation across different parts of the organisation.

Empirical material gathered through semi structured interviews and internal documentation was examined in relation to each clause, with the aim of determining whether the organisational practices described and documented were sufficient to satisfy the basic governance logic of the standard. Rather than applying a binary compliant or noncompliant classification, the gap analysis employs three levels of assessment. Practices that meaningfully satisfy the requirements of a given clause and provide a foundation upon which a compliant system could be built are classified as substantially aligned. Practices where relevant structures or instruments exist but where

the scope, formalisation or institutional embeddedness falls short of full compliance are classified as partially aligned. Areas where the requirements of the standard are either absent from current practice or where existing structures are sufficiently misaligned that incremental development would be insufficient to achieve conformance are classified as areas of significant nonconformance.

This three level assessment structure enables a differentiated analysis that reflects the actual variation in supply chain security maturity across the organisation, rather than reducing the assessment to a single compliance score. As Yin (2018) argues, analytical frameworks applied within case study designs should be sufficiently structured to enable systematic comparison while remaining responsive to the complexity and context of the case under examination. The analytical process involved examining interview data and internal documentation in parallel, assessing how practices were both formally described in documented structures and understood in practice by organisational members. Discrepancies between documented procedures and their operational application were treated as analytically significant, consistent with Bryman's (2016) argument that the combination of different qualitative data sources enables a more comprehensive understanding of both formally expressed structures and their enactment in organisational practice.

3. Literature Framework

The chapter establishes the theoretical foundation of the analysis. It covers supply chain security as a research field, security governance in complex supply chains, risk management in upstream supply chains and management systems as a form of organisational formalisation. ISO 28000 and its clause structure are then presented as the analytical reference framework applied throughout the analysis.

3.1 Supply Chain Security

Supply chain security has developed into a distinct field of research as global supply networks have grown increasingly complex, geographically dispersed and interdependent. The expansion of multi tier supplier structures, outsourcing of critical components and dependence on international logistics infrastructure have increased exposure to vulnerabilities that extend beyond individual organisations. Early studies defined supply chain security as the protection of material flows, information systems and infrastructure against intentional acts such as terrorism, theft, sabotage and organised crime (Williams, Lueg & LeMay, 2008). This perspective emphasised the need to protect goods and transportation systems from malicious interference, especially after major geopolitical events that demonstrated how supply chains could be exploited to cause widespread societal and economic consequences. Over time, the concept has expanded to include broader governance mechanisms that integrate security into organisational strategies and operational routines, reflecting the increasing interconnection between the physical, informational and organisational dimensions of supply networks (Thomas & Vaduva, 2015).

As supply chains have become more complex in structure, the boundary between supply chain security and supply chain risk management has become more integrated. In the literature on supply chain risk management, risk is described as the probability and consequences of events that disrupt supply chain flows and reduce operational performance (Ho, Zheng, Yildiz & Talluri, 2015). Within this broader risk management perspective, security threats constitute a specific risk category characterised by intentionality and strategic focus. Ghadge, Dani & Kalawsky (2012) emphasise that supply chain risk management requires systematic processes for identification, assessment and mitigation supported by organisational structures and decision making frameworks. Security management could therefore be understood as a specialised application of these risk management principles, focusing on threats arising from intentional actions rather than operational variability. This positioning places supply chain security within structured governance processes rather than as a purely technical or reactive function.

The systemic characteristics of supply chain security is further reinforced by research examining dependencies between organisations and cascading disruption effects.

Supply networks consist of interconnected nodes where upstream disruptions spread via logistics interfaces and downstream partners. Spieske and Birkel (2021) suggest that disruptions in the supply chain often give rise to ripple effects that extend across multiple levels, especially when transparency and coordination mechanisms are limited. Security vulnerabilities are often embedded in these structural characteristics, as limited visibility beyond first tier suppliers may obscure exposure to political instability, regulatory uncertainty or malicious interference. In this context, supply chain security requires coordination mechanisms that increase transparency, enable monitoring and clarify responsibilities across organisational boundaries. Security management must be integrated into logistics planning, supplier evaluation and information management to reduce systemic exposure (Thomas and Vaduva, 2015). Security is thus presented as a cross functional management area embedded within the architecture of supply chain management. A further dimension emphasised in recent studies concerns organisational capacity in relation to supply chain security. Maturity in risk management as a development process in which structured routines, defined roles and continuous evaluation mechanisms strengthen organisational performance (Żurawski et al., 2025). Applied to the supply chain, this means that security effectiveness depends on the institutionalisation of procedures rather than on isolated protective measures. Ho et al. (2015) emphasise that effective risk management frameworks integrate identification, assessment, risk reduction and monitoring into repeatable organisational processes. When these principles are applied to security management, the result is a structured system with documented procedures, evaluation criteria and accountability structures that enable consistent application across all supplier relationships. This capability based perspective reinforces the idea that supply chain security is maintained through governance structures that support continuous evaluation and improvement.

Supply chain security is not limited to protecting physical goods during transport, but also covers information flows, digital infrastructure, intangible assets and the organisation's reputation. Williams et al. (2008) note that security threats are increasingly targeting information systems and network interfaces, which could jeopardise both operational continuity and stakeholder confidence. Ghadge et al. (2012) similarly argue that modern risk environments in the supply chain are multidimensional and involve technical, geopolitical, financial and relational factors that interact in complex ways. These overlapping areas increase the strategic relevance of security management, as vulnerabilities in one area could trigger chain reactions that affect operations and reputation. From this perspective, supply chain security becomes a mechanism for preserving both operational stability and long term strategic positioning in competitive and uncertain environments.

3.2 Security Governance in Complex Supply Chains

Modern supply chains operate as interconnected networks of organisations characterised by distributed decision making, resource interdependencies and multi tier

supplier structures. These structural characteristics increase exposure to disruptions that could spread across organisational boundaries and affect operational continuity (Christopher & Peck, 2004). As supply networks expand in geographical scope and complexity, the governance of risks and dependencies becomes a central organisational concern.

Governance in supply chains refers to the formal and informal mechanisms through which responsibilities, coordination and control are structured across participating actors. Christopher and Peck (2004) emphasise that vulnerability within supply chains is closely linked to structural complexity and insufficient transparency between levels. Effective governance therefore requires clearly defined roles, structured coordination and mechanisms for information sharing that enable early identification of disruptions. The establishment of such governance structures supports stability and resilience in environments characterised by uncertainty.

From a supplier network perspective, risk management in interorganisational networks demands systematic processes for risk identification, evaluation and mitigation (Hallikas et al., 2004). Supplier networks involve mutual dependencies where disruptions within one area may generate consequences across multiple partners. Governance structures must therefore include joint risk assessment processes and defined areas of responsibility that extend beyond individual organisational units. Tummala and Schoenherr (2011) further support this perspective by presenting structured supply chain risk management processes that integrate identification, assessment and mitigation into formalised organisational routines. The integration of systematic processes for risk identification, evaluation and mitigation into formalised organisational routines is necessary, highlighting the need for structured risk governance in upstream supply networks (Hallikas et al., 2004).

Cooperation between organisations constitutes an additional dimension of governance. Structured cooperation improves collective performance by strengthening information exchange, process synchronisation and coordinated decision making (Cao and Zhang, 2011). Relational capabilities and coordination mechanisms contribute to collective monitoring and transparency throughout the supply chain. Wieland and Wallenburg (2013) similarly emphasise the importance of relational competencies in building resilience and show that collaboration, trust and integration between organisations strengthen adaptability. The coordination of governance structures and relationship mechanisms therefore supports both stability and coordinated efforts in complex supply networks.

The management of complex supply chains is characterised by formalised structures, defined areas of responsibility and relationship integration across organisational boundaries. These elements ensure that supply chains function effectively and resiliently, even in situations of uncertainty and disruption. Formalised structures

provide a clear framework for decision making and accountability, while defined areas of responsibility help to avoid overlaps and gaps, promoting clarity and efficiency. Relationship integration promotes cooperation and trust between stakeholders, facilitating smoother information exchange and collective problem solving. This integrated approach to governance is essential for managing the intricate network of interdependencies that characterises modern supply chains. Structural complexity increases exposure to cascading disruptions, underscoring the need for systematic coordination and joint oversight (Christopher & Peck, 2004; Hallikas et al., 2004). The institutionalisation of risk management practices and collaborative mechanisms is fundamental to structured security governance in upstream supply chains. These governance structures create the organisational conditions for coordinated monitoring and control across the entire supply network. Within such structures, risk management is a central operational mechanism for identifying, assessing and reducing vulnerabilities. The formalisation of risk processes is therefore crucial for translating governance principles into practical security management within upstream supply chains.

3.3 Risk Management in Upstream Supply Chains

Risk management constitutes a central operational dimension of governance within complex supply networks. As supply chains extend across organisational and geographical boundaries, exposure to uncertainty increases, particularly in upstream tiers where visibility is often limited. Supply chain risk management is defined as the identification and management of risks within the supply chain and through coordination among supply chain members in order to reduce overall vulnerability (Jüttner, Peck and Christopher, 2003). This definition emphasises that risk management is not confined to individual firms but involves inter organisational coordination aimed at protecting the continuity of supply chain flows.

Various categories of risk sources influence upstream exposure. These include environmental risk sources, organisational risk sources and network related risk sources (Jüttner et al., 2003). Environmental risks originate from external factors beyond the supply chain, such as geopolitical instability and external disruptions. Organisational risks arise within individual firms, including operational failures or internal process breakdowns. Network related risks originate from interactions among supply chain actors and are particularly relevant in upstream structures characterised by outsourcing, supplier concentration and multi tier dependencies. Hallikas et al. (2004) describes that supplier networks involve mutual dependencies where disruptions may propagate across interconnected actors. Consequently, limited transparency beyond first tier suppliers further increases the difficulty of identifying and evaluating such network related vulnerabilities.

Structured risk management processes have been proposed as a means of addressing these upstream exposures. Tummala and Schoenherr (2011) present a systematic supply

chain risk management process that integrates risk identification, assessment, evaluation and mitigation into formal organisational routines. The framework emphasises the importance of consistent methodologies for evaluating likelihood and impact across supplier relationships. Formalised risk processes enhance comparability between suppliers and support prioritisation of mitigation efforts based on assessed exposure levels. Additionally, variations in supply chain risk exposure are associated with differences in operational performance, indicating the direct organisational impact of upstream risk management (Wagner and Bode, 2008).

Risk management in upstream supply chains therefore extends beyond isolated assessment activities. Jüttner et al. (2003) emphasise that effective supply chain risk management requires coordination among supply chain members to reduce collective vulnerability. This coordination involves defined responsibilities, shared risk awareness and mechanisms for structured information exchange. Hallikas et al. (2004) note that risk assessment becomes increasingly complex across multiple supplier tiers, where the appropriate scope of analysis may be difficult to determine. The absence of structured approaches may result in fragmented risk perception and inconsistent mitigation efforts across organisational interfaces.

3.4 Management Systems and Organisational Formalisation

Management systems constitute structured organisational frameworks through which policies, objectives and processes are formalised and integrated into operational practice. International management system standards define documented requirements that guide how organisations plan, implement, monitor and improve their activities. These systems institutionalise responsibilities, procedures and performance evaluation mechanisms in order to enhance transparency, traceability and control (Fonseca et al., 2017). Through certification mechanisms, organisations are able to demonstrate alignment with externally defined requirements, which strengthens both internal coordination and external credibility. The adoption of management system standards contributes to organisational formalisation by clarifying structural arrangements and embedding systematic routines across functional domains. Domingues et al. (2016) argue that integrated management systems enhance organisational coherence by aligning processes and reducing fragmentation between departments. Formalisation enables harmonisation of procedures that might otherwise be developed independently, thereby strengthening systemic consistency. This structured integration supports managerial oversight and promotes coordinated decision making across organisational units.

Integrated management systems stress the importance of systemic management and standardisation as fundamental principles for organisational development. Nunhes et al. (2019) identify systemic alignment, process standardisation and strategic integration as key pillars underlying successful management system implementation. Standardisation in this context extends beyond documentation and includes the

alignment of terminology, evaluation criteria and operational routines. The institutionalisation of such structures enhances organisational maturity by embedding recurring evaluation and feedback mechanisms within everyday activities. Contemporary ISO management system standards are commonly structured around the Plan-Do-Check-Act (PDCA) logic, which integrates planning, execution, performance evaluation and continuous improvement into a recurring cycle. The adoption of the high level structure across ISO standards facilitates integration between different management domains by harmonising core clause structures and terminology (Fonseca et al., 2017). This structural convergence enables organisations to integrate quality, environmental, safety and security domains within a unified governance architecture.

Certification and system integration yield both internal and external organisational effects. Management system certification is linked to enhancements in process control, performance monitoring and stakeholder confidence (Fonseca et al., 2017). Formalised management systems thus serve as governance infrastructures that institutionalise structured processes, enabling systematic evaluation and improvement. Maturity in integrated systems supports organisational capability by embedding structured routines and performance review mechanisms (Domingues et al., 2016). These systems translate governance principles into formalised structures, documented procedures and recurring improvement cycles. Through standardisation, integration and performance monitoring, they establish the structural foundation necessary for coordinated governance across complex organisational domains. This conceptualisation offers the theoretical basis for understanding ISO 28000 as a specialised security management system within the broader family of international management standards.

3.5 ISO 28000 as an Operational Framework

Supply chain security has been conceptualised as the structured application of policies, procedures and technologies aimed at protecting assets, flows and continuity within supply networks. Within the broader framework of supply chain risk management, security represents a targeted mitigation strategy addressing intentional disruptions, vulnerabilities and threats that may affect organisational performance and network stability (Williams et al., 2008). Effective security management requires integration across organisational functions and coordination with supply chain partners, rather than isolated protective measures. This conceptual positioning creates a need for formalised governance mechanisms capable of translating security principles into systematic organisational practice. ISO 28000 responds to this need by establishing a standardised management system structure designed specifically for supply chain security (ISO, 2022; Williams et al., 2008).

ISO 28000 (ISO, 2022) specifies requirements for establishing, implementing, maintaining and continually improving a security management system applicable to supply chain contexts. The standard adopts a risk based management system structure aligned with other ISO standards, thereby enabling integration with existing

governance systems and organisational control mechanisms. It requires organisations to define the scope of the system, analyse internal and external contextual factors, identify relevant stakeholders and establish a security policy endorsed by top management (ISO, 2022). This formalisation institutionalises supply chain security within organisational governance structures and clarifies responsibility at the leadership level. Thus, this aligns with the argument that security must be embedded in strategic management processes rather than treated as an operational afterthought (Williams et al., 2008). A core component of ISO 28000 is the systematic identification and assessment of security risks. Organisations are required to identify threats, assess vulnerabilities, evaluate potential consequences and determine appropriate control measures based on documented criteria (ISO, 2022). This requirement operationalises the supply chain risk management logic described by Williams et al. (2008), where security functions as a mitigation mechanism within a broader risk governance framework. In requiring structured risk assessments and traceable decision processes, the standard transforms abstract discussions of vulnerability and disruption into formalised organisational routines. The risk based structure ensures that security measures are proportionate, documented and linked to defined objectives, thereby enhancing transparency and consistency across the supply chain (ISO, 2022; Williams et al., 2008).

ISO 28000 further requires defined roles, responsibilities, competence requirements, communication processes, operational controls and documented procedures covering internal operations as well as supplier and logistics interfaces (ISO, 2022). This extends security management beyond internal processes to include upstream and downstream actors, reflecting the interorganisational dimension of supply chain security emphasised in the literature (Williams et al., 2008). The standard requires organisations to monitor performance, conduct internal audits, perform management reviews and implement corrective actions to address identified deficiencies (ISO, 2022). These requirements create a structured governance cycle in which security is continuously evaluated and improved. The embedded continuous improvement logic ensures that security management evolves in response to changing threat environments and organisational conditions and thereby reinforcing adaptive capacity within supply networks (ISO, 2022; Williams et al., 2008).

The industry's adoption of ISO 28000 is driven by perceived benefits related to structured risk management, improved documentation practices, enhanced stakeholder confidence and strengthened coordination across supply chain actors. It contributes to clearer internal processes, increased transparency and greater credibility in relation to customers and regulatory authorities (Ing et al., 2019). This supports the theoretical argument that formalised management systems provide governance clarity and reduce ambiguity in the interpretation and application of security requirements (Williams et al., 2008). In this sense, ISO 28000 functions as an operational framework that aligns strategic security objectives with documented procedures, measurable targets and

systematic review mechanisms (ISO, 2022; Ing et al., 2019). More broadly, the standard provides a structured and auditable mechanism for translating theoretical principles of risk mitigation and supply chain network protection into coherent organisational practice, thereby embedding abstract security concepts within formalised governance structures (Williams et al., 2008; Ing et al., 2019). Through its system oriented structure, ISO 28000 establishes supply chain security as a sustained governance function embedded in both strategic and operational decision making processes (ISO, 2022; Williams et al., 2008).

3.5.1 ISO 28000 Clause Framework

ISO 28000 follows the standardised high level structure and is built around the PDCA framework (ISO, 2022). This approach frames security management as an integrated management system, where context analysis, strategic alignment, risk based planning, operational execution, monitoring and continual improvement are systematically interconnected. The standard thus not only specifies a set of security measures but also establishes a model for how security should be formalised and institutionalised organisationally.

3.5.1.1 Clause on Context of The Organisation

The organisation is required to identify internal and external factors that may influence the security management system's ability to achieve its intended outcomes, as well as to determine relevant stakeholders and their needs and expectations (ISO, 2022). In addition, the scope of the system must be clearly defined and documented. These requirements frame security as both context dependent and relational. Elements such as the organisation's external environment, regulatory landscape, business model and dependencies on suppliers form an integral part of the management system's foundation. Accordingly, security management relies on explicitly defined boundaries and a clear understanding of stakeholder interdependencies, ensuring that the system is structured in alignment with its organisational and environmental context.

3.5.1.2 Clause of Leadership

Top management is required to demonstrate responsibility and commitment to the security management system (ISO, 2022). This includes establishing a security policy, ensuring that security objectives are defined and clearly assigning roles and responsibilities. Through these measures, security governance is embedded at a strategic level and supported by a formal allocation of authority and accountability. Security is thereby framed as a managerial concern and integrated into the organisation's broader governance framework. In this way, leadership authority and organisational accountability are formally established, ensuring that security is directed, supported and sustained at the highest level of management.

3.5.1.3 Clause on Planning

The organisation is required to apply a risk based approach by identifying, analysing and evaluating security related risks, followed by planning appropriate measures to address them (ISO, 2022). Risk management must be conducted systematically and in proportion to identified threats and vulnerabilities. By connecting risk assessments to defined objectives and planned actions, security governance is framed as a structured and informed decision making process. In this way, uncertainty and potential threats are translated into prioritised actions and formalised governance decisions within the management system.

3.5.1.4 Clause on Support

Adequate resources must be provided and requirements concerning competence, awareness, communication and the control of documented information must be fulfilled (ISO, 2022). Personnel are expected to possess the necessary skills and knowledge, while documentation is to be properly managed and protected. Through these measures, security related activities are embedded within formal organisational structures. Knowledge management, responsibilities and information handling are systematised and made independent of individual actors. As a result, security management becomes integrated into the organisation's enduring systems and operational routines, ensuring continuity and consistency over time.

3.5.1.5 Clause on Operation

Operational implementation of the security management system requires that necessary processes be planned, executed and controlled in order to address identified risks, including those related to suppliers (ISO, 2022). Strategic intentions and planning are thereby translated into concrete organisational practices. Operational controls, risk treatment measures and security plans must be documented and aligned with the level of identified risk. In this manner, overarching management principles are systematically converted into structured procedures and measurable control activities within the organisation.

3.5.1.6 Clause on Performance Evaluation

Monitoring and measurement of security performance are required, along with the conduct of internal audits and regular management reviews (ISO, 2022). These mechanisms establish a structured process of feedback and evaluation. Security management is thereby subjected to systematic internal control and ongoing assessment. Through these arrangements, the effectiveness and performance of the system are continuously examined, promoting accountability and organisational transparency.

3.5.1.7 Clause on Improvement

Requirements are established for addressing nonconformities and ensuring continuous improvement (ISO, 2022). Causes of identified nonconformities must be determined

and appropriate corrective actions implemented. By embedding improvement processes within the management system, security management is structured to remain adaptive and responsive. In this way, the system is continuously refined in light of experience, evaluation results and evolving internal and external conditions.

4. Empirical Data from The Company

The chapter describes the organisation and its current approach to supply chain security. It presents how security is organised, how suppliers are classified and managed as well as how processes for risk assessment, incident management, competence development and performance evaluation are structured and applied in practice.

4.1 Company Description

The company is an established actor within the defence and security sector, providing integrated technological systems for military and civil security applications. Its portfolio encompasses a comprehensive range of advanced systems and technologies, developed to address varied and demanding operational contexts (Company X, 2025). These offerings are developed as comprehensive solutions in which mechanical structures, advanced electronics and digital functionalities are combined into fully integrated operational capabilities. The organisation's operations are structured around several functional areas that reflect its core capability domains, each operating under an overarching group functions layer that provides centralised governance, strategic direction and shared support services across the organisation. These functional areas cover a broad set of capabilities, through which the organisation delivers both complete systems and subsystems, often integrated into larger defence architectures (Company X, 2025).

Demand for the organisation's capabilities has grown substantially in recent periods, reflecting a sustained and structural shift in its market environment rather than short term fluctuations. This development is observable across the organisation’s functional areas of operation and indicates that customers are increasingly integrating the organisation’s offerings into longer term operational and strategic planning (Company X, 2025a, 2025b, 2025c & 2025d).

4.1.1 Security Management at The Company

Security constitutes a fundamental and deeply embedded dimension of the company's operations, representing not merely a compliance obligation but a core organisational value that shapes both everyday practices and broader strategic priorities. The security strategy is organised around six areas, including information security, loss prevention, personnel security, site security, supply chain security and security incidents, with the purpose of supporting operations and employees across all of these areas. This structure suggests that security is approached in a comprehensive and multidimensional manner, encompassing not only the protection of information and physical assets, but also the protection of personnel, facilities, supply networks and the organisation's ability to prevent, manage and respond to threats and incidents. Dedicated processes further support the practical security activities carried out across the various parts of the organisation, with the aim of enabling compliance with requirements and facilitating

governance and follow up. Security should therefore be understood not only as a control function, but also as an enabling capability that contributes to operational continuity, resilience and organisational credibility.

The approach to security is defined in the company's *Security Policy*, which conceptualises security as an essential and embedded component of its overall operations and business practices. The policy establishes that the organisation aims to be recognised globally as a company with high security awareness and strong professional capability in risk management. In this context, security is closely connected to business execution and to maintaining trust among customers and authorities (Company X, 2020).

Security is described as being based on structured and professional risk management practices intended to protect personnel and assets from qualified threats. The policy explicitly states that the company shall comply with all applicable security requirements, including those imposed by customers and other stakeholders, as well as legal, regulatory and contractual obligations. It further emphasises that security considerations must be integrated into all phases of operations, starting at the earliest stage of planning, ensuring that security is proactive and embedded in decision making processes (Company X, 2020).

The policy further highlights the importance of promoting a strong security culture and awareness throughout the organisation, driven from the top down by management. Continuous management of risks and vulnerabilities is emphasised as necessary to address evolving threats. Protection of assets is defined in terms of safeguarding confidentiality, integrity, availability and traceability, with measures scaled to protect both physical and digital assets. The policy also addresses preparedness through incident and crisis management, continuous monitoring, auditing and testing of compliance, as well as ongoing improvement of security related processes, methods and tools (Company X, 2020).

4.1.2 Supply Chain Security at The Company

Supply chain security at the company is described across the organisation as an emerging and developing area, the significance of which became increasingly evident during the disruptions experienced in the covid-19 pandemic. Respondent 1 states that this served as a critical turning point, exposing vulnerabilities in the supply chain as suppliers struggled with capacity shortfalls and delivery disruptions. Products that had previously not been considered critical suddenly became so, as the inability to secure them threatened its own production continuity. This prompted a recognition that security needed to expand beyond its internal organisational foundations to encompass the supplier network on which the company's operations depend.

While security has long been a central and well established dimension of the organisation's business, the specific application of security principles to the supply chain represents a newer and distinct development. As Respondent 1 describes, the rationale behind the establishment of dedicated supply chain security resources was not primarily to strengthen its own internal security posture, but to secure the supplier network itself, ensuring that the company could maintain uninterrupted production regardless of external disruptions. The emphasis has therefore shifted from the organisation alone to building a more resilient and security aware network of suppliers and partners. In this sense, the approach represents a broader ambition than operational redundancy in isolation, as the intention is to raise the security maturity of the wider partner network, making not only the organisation but also its partners more robust in the present threat environment. Respondent 1 further notes that suppliers and partners are expected to understand both the seriousness of the current security landscape and the particular responsibilities that come with being part of its supply chain.

The operational structure through which this work is conducted is captured in the *Supply Chain Security Framework*, illustrated in Figure 4. The framework organises security activities across three processes, namely assessing suppliers, procuring and managing suppliers, which together constitute the structured sequence through which security requirements are introduced, evaluated and monitored in relation to the supplier network. The principal means of communicating security obligations to suppliers are the *Supplier Code of Conduct* (SCoC), which sets out the ethical and security standards expected of all suppliers and the *Security Annex*, which establishes the specific contractual security requirements applicable to suppliers with access to the company's operations. Together these measures form the foundation for operationalising supply chain security governance across the supplier network, supported by activities aimed at raising awareness and providing training to both internal personnel and suppliers.

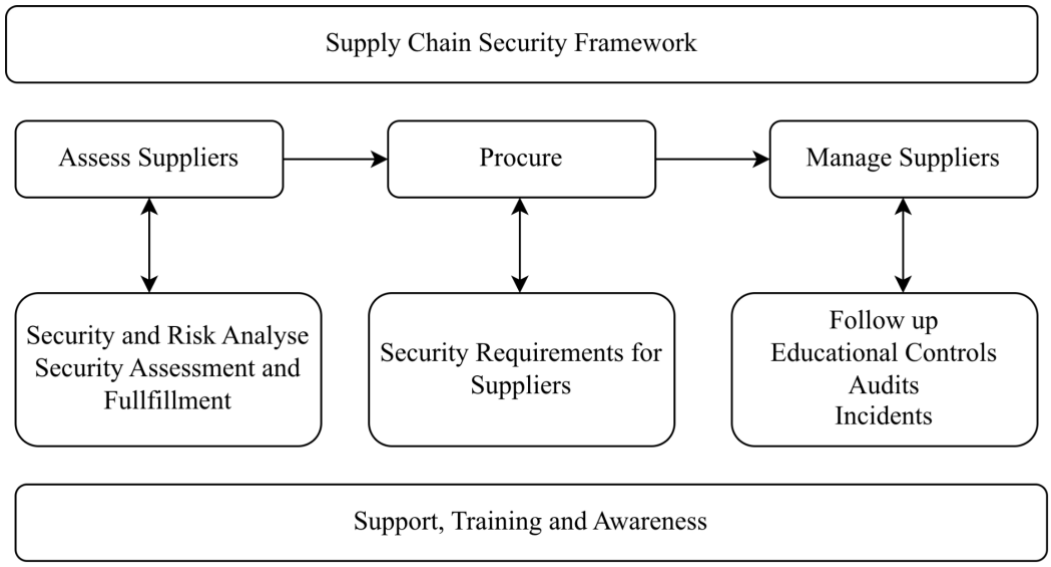

Figure 4. The Supply Chain Security Framework, depicting the three principal processes of supplier engagement and the supporting activities associated with each process.

A defining characteristic of the company's approach is that the scope and depth of security activities applied to any given supplier are not uniform but are determined by the degree to which that supplier is exposed to its security sensitive operational environment. As illustrated in Figure 5, this determination is structured around three core security dimensions, namely confidentiality, integrity and accessibility, which together define the nature and extent of a supplier's exposure to the company's operations. A supplier with access to classified information, integrated into critical production processes or involved in operationally sensitive activities will consequently be subject to a broader and more extensive set of security requirements than one that operates at the lower end of its supply chain. The security activities applied across the supplier assessment, procurement and supplier management processes are thus measured to reflect each supplier's actual exposure profile, to ensure that the extent of security engagement remains proportional to the associated risk.

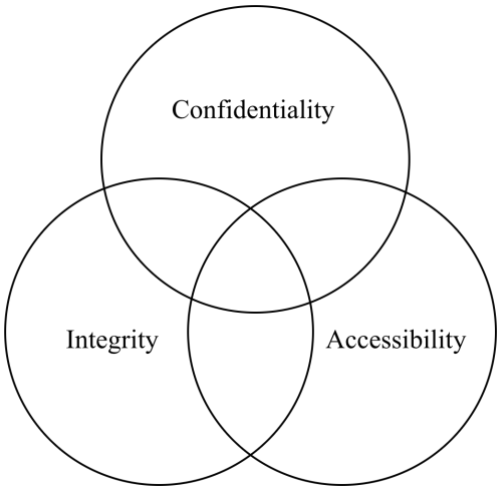

Figure 5. The Three Security Dimensions of Confidentiality, Integrity and Accessibility.

In recent years, supply chain security efforts have primarily been carried out through the establishment of requirements and the provision of training, with supply chain security functions integrated into procurement processes. Several respondents noted that dedicated supply chain security roles within the different functional areas were established only recently, suggesting that the function is still at an early stage of development. The organisational structure for supply chain security is distributed across the company's functional areas, with each area having appointed individuals responsible for supply chain security within their respective areas. Thus, the ways in which supply chain security is operationalised vary across the organisation. However, the Subject Matter Expert (SME) group acts as a central coordinating function across these distributed roles, connecting individuals involved in supply chain security from all functional areas. The group is described by multiple respondents as the primary forum for sharing experiences, discussing challenges and developing common working methods. It produces a shared standard operating procedure with defined goals and activities for the upcoming year and functions as a mechanism through which more systematic and aligned ways of working are progressively being developed. The concerned respondents emphasised the value of the SME group as a source of support and coordination in what is otherwise described as a relatively isolated function within each business area.

Despite the existence of this coordinating structure, the overall maturity of supply chain security within the organisation is described as uneven. Several respondents highlighted that engagement with supply chain security among procurement personnel varies considerably, with some purchasers demonstrating a well developed understanding of security requirements while others require more active guidance and support. The integration of supply chain security into procurement decision making processes, particularly at the earlier stages of the sourcing process, is described as limited, with security considerations often entering the process at a relatively late stage. Multiple

respondents expressed a shared view that a more proactive and earlier integration of security into procurement workflows would be beneficial, though resource constraints and competing priorities are noted as factors that currently limit the pace of development in this area.

4.1.3 Security Requirements and Organisational Awareness

The principal instruments for communicating security obligations to suppliers are the *SCoC* and the *Security Annex*. The *SCoC* constitutes a standard requirement in all supplier contracts, whereas the *Security Annex* applies only to suppliers whose engagement with the organisation entails exposure across one or more of the three security dimensions of confidentiality, integrity and accessibility, as illustrated in Figure 5. Suppliers of non critical standard products not operating within the company's security sensitive environment are thus governed solely by the standard contract and the SCoC. However, where the *Security Annex* applies, it establishes specific and more stringent security requirements that must be fulfilled throughout the contractual relationship. For strategically important suppliers, this engagement extends further, with a dedicated governance structure developed in collaboration between the company and the supplier to ensure sustained alignment on security obligations and expectations over time. Several respondents describe the *Security Annex* as comprehensive in its coverage but challenging to interpret and apply in everyday procurement processes. Respondent 5 notes that, when it was initially introduced, there was considerable frustration among procurement personnel because the requirements were extensive but few people were able to answer the questions that arose. Other respondents similarly noted that understanding how to apply it correctly has required repeated dialogue with colleagues over time.

Awareness and education activities directed at both internal procurement personnel and suppliers are conducted within the organisation. These include training and workshops for procurement employees as well as educational security controls conducted at supplier premises. Respondent 10 describes visiting suppliers to provide security education prior to contract signature, while Respondent 9 describes joint visits conducted together with procurement personnel as a means of clarifying the requirements set out in the *Security Annex*. Given the varying degrees of security exposure across the supplier base, these activities are directed primarily at suppliers of strategic importance to the company, where the security engagement is considered most appropriate. Several respondents noted, however, that even within this group, the frequency of such activities remains lower than desired and that there is still a need to further strengthen competence in supply chain security among both procurement personnel and suppliers. Also, a concern raised by several respondents is that suppliers at times sign the contractual requirements of the *Security Annex* without adequately understanding the content of those requirements. As a result, security and procurement personnel have in some cases conducted joint visits to suppliers in order to clarify the requirements and provide guidance.

4.2 Security Management System

The subsequent sections discuss the current structure and operationalisation of supply chain security within the security management system. The description is organised around the core processes and functions that collectively constitute the security management system as it is presently implemented in practice, informed by both internal organisational documentation and perspectives gathered from respondents across various functional areas and organisational functions. It addresses the definition of context and scope, the role of leadership and top management in security governance, the identification and management of risk, the organisation of support processes, the application of operational controls in procurement and supplier management, the handling and reporting of incidents as well as the evaluation of performance and pursuit of improvement.

4.2.1 Decentralised Scope Definition and Organisational Context

The approach to defining the context and scope of its security management system is structured around the principle that each functional area and business unit determines its own scope based on its specific operational context, customer requirements and contractual obligations. As described by Respondent 3, this decentralised approach is a deliberate and practically motivated structure, necessary to ensure that the scope definition remains applicable and meaningful across the organisation's diverse operational contexts. This is reflected in the *Security Operations Manual* (INF-0506), which provides the overarching structure for how the security management system is established and maintained across the whole organisation, while explicitly allowing individual areas and units to define their own boundaries and applicability based on their respective contexts. Respondent 3 further notes that the manual describes how the current security management system is structured in alignment with ISO 27001, meaning that existing processes and tools for scope definition and context analysis are primarily developed in relation to this standard.

To support functional areas and units in understanding their organisational context, the organisation provides a dedicated guidance document, *Understanding the Organisation and its Context* (INF-1223), which assists organisational units in identifying internal and external issues relevant to their purpose and strategic direction. This document is connected to the *Interested Parties Analysis* (INF-0646), which guides organisational units in identifying relevant stakeholders and assessing their requirements across quality, environment, occupational health and safety and security dimensions. A standardised template (5000362-359) is used for conducting these analyses, covering aspects such as interested parties groups, their requirements, compliance obligations and their importance to the management system. The results of these analyses are intended to be monitored and reviewed through the management review process.

In practice, the definition of scope and context for supply chain security is not determined at a corporate level. The operational contexts across the organisation differ considerably, as factors such as customer requirements, local regulations and contracts vary significantly between areas, making a uniform top down scope definition impractical. Respondent 3 describes that each functional area is therefore responsible for conducting its own analysis and determining the boundaries within which its security management system applies. The scope of the security management system is furthermore considered a decisive factor for achieving meaningful outcomes in security management activities. Respondent 7 notes from prior experience that an excessively broad scope creates challenges in terms of mapping and prioritisation, as the scope is most effective when driven from business needs and customer requirements rather than defined at an organisational level that is too large to be practically manageable.

4.2.2 Governance Structures and Decision Making Authority

Leadership and governance within the security management system is structured through a set of formally established processes and documents that define how responsibilities are distributed and how management oversight is exercised throughout the organisation. The overall governance of the organisation's global management system is described in the *Governance of The Global Management System* (WHO-0070), which outlines the different roles, teams and organisational units that collectively form the global management system governance structure. This document establishes the formal basis through which leadership responsibilities are distributed across the organisation, though its scope covers the broader management system rather than supply chain security specifically.

Top management commitment to security is expressed through the organisation's *Security Policy* (WHY-0018), which establishes security as a central organisational principle and assigns overall accountability for security outcomes at the leadership level. Roles and responsibilities within the security management system are formally defined through the *Security Operations Manual* (INF-0506), which distributes responsibilities using the RAPID method. RAPID is a decision making tool used to clarify organisational responsibilities by defining who recommends, agrees, performs, inputs and decides in relation to a given process or decision. This structure is further complemented by the role definition document (INF-0512), which describes each role from CEO level to document and information owner level, clarifying who holds responsibility over specific processes and decisions. However, respondent 3 describes these structures as primarily developed in relation to the existing security management system aligned with ISO 27001.

Respondent 1 identifies different levels within top management, these describe the critical decision making process and notes that two different groups make decisions regarding more critical procurements. For simpler procurements, decisions are made at individual or operational level, but for critical procurements, decisions are escalated.

At the first level is the *Sourcing Council*, which convenes procurement managers, legal representatives and individuals responsible for supply chain security and serves as the setting where strategic decisions are made and more complex issues that cannot be resolved at an operational level. *Terms of Reference for the Procurement Council* (WHO-1882) composition, formally defines roles and mandate which establishes the responsibilities and decision making authorities for each role represented within the council. The *Sourcing Council* could also escalate decisions, which are then made by the *Sourcing Board*, where the most critical decisions must be made.

Management engagement with the broader security management system is further structured through the management review process (HOW-0018), the purpose of which is to enable a regular and systematic review of management system performance beyond the immediate demands of everyday operations. At group functions level, this process is described more carefully in the *Management Review at Group Functions* document (INF-1708). Reviews are conducted on a quarterly basis following the *Annual Planning Wheel* (GMS-0275), see figure 6, where the first quarter is used to examine the results of the previous year's review, the second and third quarters are used to make adjustments and refinements and a new review is conducted in the fourth quarter. These reviews are held at minimum twice a year at group functions level and are intended to ensure the continuing suitability, adequacy and effectiveness of the security management system. The management review process as it currently operates is however structured around the broader security management system and does not include a specific focus on supply chain security.

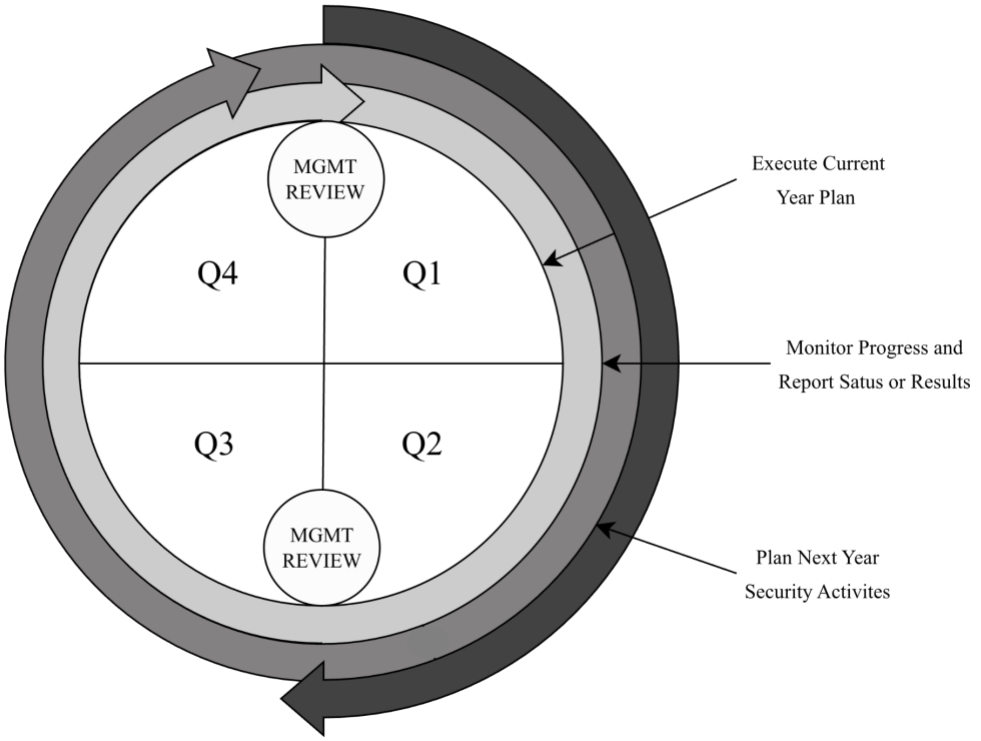

Figure 6. The Security Annual Wheel illustrates the yearly plan, execute and monitor cycle.

4.2.3 Risk Assessment and Supplier Classification

Risk management within the company is founded on the guidance provided by ISO 31000, the international standard for risk management. The different functional areas, operational countries and group functions are responsible for identifying and managing risks in accordance with the group's common risk processes and current policies, guidelines and instructions. The general governance for managing risks and opportunities across the organisation is established through the process *Manage Risk and Opportunity* (HOW-0025). This provides a structured and generic approach applicable to all types of risk and opportunity situations, with different criteria applied depending on the organisational context.

A more specific measurement for proactive security risk management is the *Security Risk Assessment* process (INF-0513), which is intended to support structured and proactive security risk management across the organisation. The process consists of five steps covering planning, identification, analysis, management as well as reporting, this is intended to be conducted at planned intervals and whenever significant changes occur within the organisation. The security risk assessment process is applied primarily at the business unit level, with supply chain security expertise incorporated where assessments concern supplier relationships or other matters relevant to supply chain security.

The most consistently applied risk management tool within supply chain security is the risk and sanction screening process, which is mandatory for every procurement process. The screening is conducted using external databases and covers six risk domains, examining sanctions against the company itself, sanctions against owners, percentage of state ownership, connections to political exposure, negative media coverage and other official lists. As described by Respondent 11, the screening process is standardised and initiated through a form submitted by the purchasing officer, with information about the supplier, description of needs and the reason for the screening. A more detailed description from the purchasing officer enables the risk team to focus on the most relevant aspects of the assessment. The screening process operates in two phases. An initial screening is conducted prior to the second decision point in the procurement process and before a supplier is selected. Following contract signature, a continuous monitoring process is established whereby suppliers are regularly checked against the same sanction and risk lists. If the risk team identifies a match against any of the six risk domains, an internal escalation process is initiated. Thus, if the risk team cannot make the assessment independently, the matter is escalated to the export control function and as a final step to an external law firm if required. Respondent 11 further describes that screening has been extended beyond first tier suppliers in certain cases, where the company procures through distributors and screening is also conducted against the manufacturer of the product in question. While this currently only occurs during the initial screening phase, a register is being developed to enable continuous monitoring of these manufacturers as well.

Beyond the mandatory screening process, risk management in supplier relationships is further shaped by customer requirements and the *Security Annex*, both of which impose additional security obligations on suppliers that are exposed to the organisation's operations, sensitive information or critical assets, as illustrated in Figure 5. The current classification of suppliers is based on the Kraljic matrix, a classification that is not specifically designed to reflect security related risk dimensions such as the nature of information shared with the supplier, ownership structures or the organisation's dependency on the supplier, as noted by Respondent 7. Respondent 12 additionally raises the issue of aggregated data, noting that a supplier receiving small amounts of information over an extended period may gradually accumulate a level of sensitive knowledge that would warrant higher security requirements and that this dimension is not always captured in the current approach to supplier classification. Respondent 1 describes an ongoing effort to introduce a classification of high security business impact (HSBI) suppliers. The initiative aims to differentiate suppliers based on the scope of their exposure to the company's operations, with the intention of identifying which suppliers warrant elevated security governance beyond what is determined by their existing classification in the Kraljic matrix. Supporting instructions are currently being developed and security considerations are expected to be integrated earlier in procurement processes involving HSBI suppliers, with requirements to be imposed on

procurement personnel accordingly. Multiple sources emphasises the broader risk management activities outside of the mandatory screening process are described across the organisation as less systematic. Thus, risk processes and analyses beyond the screening are less clearly defined in terms of working methods and responsibilities, representing an area where further development is considered necessary.

4.2.4 Support Processes and Competence Development

There are no formally defined competence requirements for those involved in supply chain security. Individuals currently in supply chain security roles across different functional areas have a variety of professional backgrounds and the competencies required for such roles have not been formally specified or documented at an organisational level. As emphasised by Respondent 10, supply chain security requires a broad set of skills and developing competence in this area both among internal procurement personnel and within the supplier base is an ongoing priority. Throughout the organisation, the level of understanding among procurement personnel varies considerably between individuals and functional areas and the need to strengthen competence in supply chain security is a recurring observation.

The ongoing *Security Awareness Programme* (INF-0605) is responsible for managing security awareness across the organisation, with the central security function holding overall responsibility. This includes the coordination and administration of the organisation's common awareness content, as well as its maintenance and development, to ensure access to mandatory corporate training. The awareness program informs personnel of changes to policies, reminds staff of existing requirements and draws attention to security issues that may affect the company's operations. At the point of employment, security awareness is incorporated into the onboarding process, covering relevant security policies and procedures. The security portal and the corporate intranet are additionally used to communicate important security information and updates to personnel throughout the organisation. As described by Respondent 1, supply chain security awareness directed specifically at procurement personnel is described across the organisation as an area requiring further development, with training activities currently occurring less frequently than considered necessary.

Communication within the security management system is supported by the guidelines document *Manage Communication* (INF-0620), which provides a structured framework for both internal and external communication based on the RAPID method. The guidelines specify with whom communication should occur, when and how, with guidance on managing different types of information across different recipient groups and situations, which covers both internal and external communication relevant to security matters. The management of documented information across the organisation follows the process *Manage Information* (HOW-0089), which applies uniformly to all documented information. All documents are subject to formal requirements regarding identification, including title, release date and owner, as governed by the document

Marking of Information (INF-0502), which also addresses the handling of documents subject to export control or elevated sensitivity classifications.

Multiple respondents describe a forthcoming enterprise resource planning initiative referred to as Spark, which is currently under development and not yet implemented. When implemented, Spark will introduce a unified system across all areas and units, enabling purchasing officers to identify existing contracts with a given supplier across the organisation without needing to initiate a new procurement process. Several respondents describe this as a significant development that is expected to increase process efficiency and consistency across the organisation, as procurement decisions and supplier information will be consolidated within a single shared system. It is also noted that security could be improved, as all steps in the procurement process would require approval before proceeding, whereas buyers currently only need approval at decision points.

4.2.5 Security Controls in Procurement and Supplier Management

Supply chain security is operationalised primarily at the supplier network level, where security requirements are introduced, assessed and followed up across supplier relationships through a structured set of controls embedded within procurement and supplier management processes. The procurement process is structured around four decision points, referred to as P1 through P4, which define the stages at which specific actions, assessments and approvals are required before proceeding. A dedicated checklist document (5000358-093) outlines the requirements applicable at each decision point and functions as a structured reference for procurement personnel throughout the sourcing process. Additionally, supplier scorecards are used in the procurement decision at P2, providing a structured assessment of supplier risk based on a set of defined criteria. As described by Respondent 14, the scorecards are owned by the security function, which retains the authority to restrict engagement with certain suppliers based on the identified risk level. Furthermore, a central operational document supporting procurement personnel is the *Corporate Purchase Agreement Templates* (INF-0380), which contains both guidance and checklists for procurement activities. This includes references to requirements such as the *SCoC* and the *Security Annex*, which point procurement personnel towards the relevant contractual instruments at the appropriate stages of the process. The *Supplier Assessment Decision Record* (5000358-247) is used to document supplier assessments. As noted by Respondent 4, efforts are currently being made to strengthen its content and references, which includes a more explicit incorporation of security considerations.

The *Security Annex* constitutes the primary contractual instrument through which security requirements are imposed on suppliers. It is included in supplier agreements if applicable and sets out the specific security obligations that suppliers are expected to fulfil throughout the duration of the contractual relationship. Supplier classification is currently based on the Kraljic matrix. Respondent 7 notes that this classification does

not incorporate security specific dimensions and Respondent 12 raises the concern that suppliers receiving limited information over an extended period may gradually accumulate sensitive knowledge that the current classification does not account for.

Security audits are conducted both internally and at supplier premises as part of the applied operational controls. Internal audit activities are governed by the *Manage Audits Programme* (HOW-0019) and the *Group Internal Audit Instructions* (INF-0641), which describe how audit objectives, scope and criteria are determined and how audit teams are assigned. Security audits and security check ups directed at suppliers are described in *Security Audit and Check-Up Process for Suppliers* INF-0596. As described by Respondent 10, educational security controls are conducted at supplier premises, with a focus on security awareness and compliance with contractual security requirements, often in connection with upcoming contracts or contract renewals. Respondent 1 emphasises that audit and control activities directed at suppliers are however not conducted systematically across the organisation and the frequency of such activities is limited by available resources across the functional areas.

4.2.6 Incident Management and Reporting

Incident management within the security management system is governed by the process *Manage Security Incidents* (HOW-0147), which provides guidelines for how security incidents are to be handled throughout the organisation. As described by Respondent 1, the process includes security incidents broadly rather than being specifically designed for supply chain security incidents, meaning that supply chain security related incidents are managed within the same general incident management structure as other types of security incidents. The process emphasises the importance of defining and communicating a clear plan for handling incidents and is closely linked to the broader processes for error and problem handling within the organisation. Documentation of incident related actions and findings is managed in accordance with the process *Manage Information* (HOW-0089).

Contractual arrangements with suppliers include information for reporting and communicating security incidents and concerns. Suppliers are expected to know how and to whom incidents must be reported to the company and this is reflected in each supplier’s contractual documentation. In practice, several respondents describe that each supplier is assigned a designated contact person at the company who serves as the formal point of contact for communication concerning security matters and incidents throughout the supplier relationship. Reporting of concerns and irregularities is further supported through the organisation's *Whistleblowing Policy* (WHY-0035), which provides a channel for raising concerns related to potential violations of the *SCoC* and other security related matters. The whistleblowing channel is available to both internal personnel and external parties, including suppliers, meaning that suppliers have access to a formal mechanism through which concerns related to security obligations and conduct could be reported. The *SCoC* explicitly references this channel, directing

suppliers to use it when concerns arise in relation to the requirements set out in that document.

Internal findings identified through audits or other means are documented and tracked in accordance with the process *Handle Operational Findings* (HOW-0031), which establishes a systematic approach for registration, classification and follow up on findings until resolved. Audit results are incorporated into the *Management Review* process (HOW-0018), reviewed twice a year at the group function level and support continuous improvement within the PDCA cycle.

4.2.7 Performance Evaluation and Development of Security Improvement

Performance evaluation within the security management system is structured around a set of established processes for monitoring, auditing and reviewing security related activities across the organisation. The overarching framework for performance evaluation is governed by the *Management Review* process (HOW-0018), the purpose of which is to follow up the management system in order to ensure its continuing suitability, adequacy and effectiveness. The management review is conducted at planned intervals on multiple levels, where results from lower levels serve as input to reviews, ultimately compiled at the company group level. As described by Respondent 1, the management review covers the broader security management system and includes supply chain security as part of this wider scope rather than as a distinct area of evaluation. Inputs to the management review include results from security audits, security incidents, security measurements, risk status and risk treatment plans, as well as the evaluation of security objectives. The *Security Annual Wheel* (GMS-0534) is a structured planning model that aligns security management activities with the organisation's broader planning cycle on a quarterly basis, ensuring performance evaluation and improvement are synchronised with overall business planning. The annual security plan for the coming year is produced and approved by top management through the management review process, following the quarterly structure illustrated in Figure 6.

Internal audit activities constitute a central mechanism for evaluating the performance of the security management system. Audit results are uploaded into a task management system where relevant personnel are notified and applicable corrections are applied. The audit programme is regularly updated to reflect changes in risks, business priorities and regulatory requirements in *Group Internal Audit Instructions* (INF-0641). Findings identified through audits or other means are managed through the process *Handle Operational Findings* (HOW-0031), which establishes a systematic approach for registering, classifying and following up on findings until closure. Root cause analysis is used to inform corrective actions, drawing on methods such as systematic problem solving, value stream mapping and lessons learned. Security objectives are established annually with inputs from the management review and are broken down into targets updated annually and decided at the operational excellence (OPEX) board meeting in

the fourth quarter. The *Management by Objectives* process (HOW-0134) provides the structure through which objectives are tracked and broken down from the company group level.

There are no formally defined key performance indicators that exist specifically for supply chain security. While performance indicators exist within the broader security management system, these are not specifically intended to measure supply chain security performance as a distinct area. As described by Respondents 1 and 3, the organisation effectively resolves individual incidents and risks, but lacks a systematic approach to learning collectively from multiple incidents over time. A common forum for the aggregated recording and review of incidents and risks is not currently in place. Respondent 7 similarly states that there is no defined method or specific objectives for supply chain security and that activities are largely driven by requests from procurement personnel rather than guided by a proactive and systematic approach to performance evaluation.

5. Analysis

The chapter conducts the structured gap analysis against the requirements of ISO 28000. It identifies areas of substantial, partial and significant nonconformance, proposes concrete improvement measures and addresses the three research questions with reference to both empirical findings and the theoretical literature.

5.1 Gap Analysis

The gap analysis assesses the degree of alignment between the existing organisational practices and the requirements of ISO 28000. The analysis is structured around three levels of alignment, such as areas where existing practices substantially satisfy the standard's requirements, areas where relevant structures exist but fall short of full compliance and areas where material nonconformances are identified. The assessment is made at group level and acknowledges that compliance posture varies across functional areas, with certain units demonstrating a more developed approach to several requirements than the broader organisational picture would suggest. It should further be noted that this assessment reflects the organisation's current state prior to any deliberate initiative to implement ISO 28000 and that several areas assessed as partially compliant reflect the existence of general management system infrastructure that would require explicit extension to the supply chain security domain rather than the construction of entirely new systems.

5.1.1 Areas of Substantial Alignment

The assessment of the organisation's existing supply chain security practices reveals several areas where organisational structures, processes and documented procedures demonstrate a meaningful degree of alignment with the requirements of ISO 28000. While the organisation has not established a supply chain security management system explicitly structured around the standard, certain foundational elements are sufficiently developed to constitute a basis upon which a compliant system could be built. These areas are not presented as fully compliant with ISO 28000, but rather as areas where existing practices reflect the underlying governance logic of the standard and where targeted development efforts would be required to achieve full conformance.

5.1.1.1 Security Policy and Leadership as a Governance Foundation

The Security Policy (WHY-0018) establishes security as a central organisational principle, assigns overall accountability at the leadership level and commits the organisation to compliance with applicable requirements and continuous improvement. The governance of the Sourcing Council and Sourcing Board further demonstrates that critical procurement decisions involving security sensitive considerations are escalated to senior levels, reflecting a degree of embedded leadership engagement consistent with the standard's intent. The management review process (HOW-0018), conducted at minimum twice a year at group functions level, provides a structured mechanism

through which top management engages with the performance and continued suitability of the security management system. The governance structure is further supported by formally defined roles and responsibilities distributed through the RAPID method in the Security Operations Manual (INF-0506) and complemented by the role definition document (INF-0512), which clarifies accountability from CEO level to document owner level.

These elements reflect the leadership requirements articulated in the clause of leadership in ISO 28000, which requires top management to demonstrate commitment to the security management system by establishing a security policy, ensuring that security objectives are defined and clearly assigning roles and responsibilities. Fonseca et al. (2017) argue that formalised management systems serve as governance infrastructures that institutionalise structured processes and that management system maturity is linked to enhancements in process control, performance monitoring and stakeholder confidence. The existence of a documented security policy communicated across the organisation, combined with a structured management review cycle, demonstrates that the governance infrastructure necessary for a functioning security management system is present at a foundational level.

Achieving full alignment with ISO 28000 would require the security policy to explicitly address supply chain security as a distinct governance domain. The existing governance structures are primarily developed in relation to ISO 27001, meaning that the formal allocation of authority and accountability does not currently extend to supply chain security in a manner consistent with ISO 28000. Williams et al. (2008) argue that security must be embedded in strategic management processes rather than treated as an operational reflection and while the policy establishes the right intent, the absence of supply chain security as an explicitly governed area means that leadership commitment does not currently translate into the structured oversight that ISO 28000 requires. Furthermore, the management review process, while systematic, does not include supply chain security as a distinct area of evaluation, which limits its utility as a mechanism for assessing and improving supply chain security performance in line with the clause on performance evaluation.

5.1.1.2 Risk and Sanction Screening as Structured Risk Management

The risk and sanction screening process represents the most consistently applied and systematically governed control within the organisation's supply chain security function. It is standardised in its execution, covers six defined risk domains and is used both for initial screening before supplier selection and for continuous monitoring after contract signature. An established escalation structure supports the process and in selected cases the screening has been extended to manufacturers accessed through distributors, demonstrating a developing awareness of multi tier supply chain exposure.

This process reflects several core requirements of the clauses on operation and planning, which require organisations to implement and maintain structured processes for identifying and assessing security related risks arising from supplier relationships and to embed controls within procurement activities. Tummala and Schoenherr (2011) argue that formalised risk processes enhance comparability between suppliers and support the prioritisation of mitigation efforts based on assessed exposure levels, which is what the screening process achieves within its defined scope. The governance logic described by Hallikas et al. (2004), in which systematic risk identification processes are embedded in supplier network management to reduce collective vulnerability, is directly reflected in the structure of this control.

Rather than requiring the screening process itself to be redesigned, the analytical implication is that other security risk management processes should be structured to reflect its governance logic. The screening process is mandatory, systematically executed and applied both at contract initiation and as an ongoing compliance mechanism, precisely the characteristics that the clause on planning requires of a comprehensive risk governance framework. The current approach lacks an equivalent degree of systematisation for the broader range of security related risks, including physical vulnerabilities, information security threats and supplier interdependencies, that fall outside the defined scope of the screening. Ghadge et al. (2012) argue that supply chain risk management requires systematic processes for identification, assessment and mitigation supported by organisational structures and decision making frameworks. The screening process demonstrates that such systematisation is achievable within this organisation and the governance model it reflects provides a concrete reference point for how broader risk management processes could be designed and institutionalised.

5.1.1.3 Incident Management and Corrective Action Infrastructure

The company maintains a functional infrastructure for identifying, documenting, escalating and following up on security incidents. The Incident Management process (HOW-0147) links incident handling closely to broader processes for error and problem management, while the Handle Operational Findings process (HOW-0031) establishes a systematic approach for registering, classifying and following up on findings until closure, with root cause analysis used to inform corrective actions. Audit results feed into the management review cycle through this infrastructure, providing a connection between operational findings and governance level monitoring. Suppliers are further assigned a designated contact person and directed to the whistleblowing channel through the SCoC, creating a formal external reporting mechanism that extends the incident governance architecture beyond the company's organisational boundary.

Although these structures are not specifically tailored to supply chain security, the structures satisfy the standard's baseline requirements for incident response and corrective action infrastructure as articulated in the clauses on operation and

improvement. The existence of a systematic findings management process that tracks issues to closure and incorporates root cause analysis demonstrates a degree of operational maturity consistent with the continuous improvement logic embedded in ISO 28000. Christopher and Peck (2004) emphasise that effective governance requires clearly defined roles, structured coordination and mechanisms for early identification of disruptions and the existing incident management and corrective action structures provide a meaningful, if partial, foundation for this kind of governance within the supply chain security domain. To achieve full alignment with ISO 28000, the incident management process would need to be adapted to capture and systematically analyse supply chain security specific incidents as a distinct category and the corrective action process would need to be explicitly configured to address supply chain security nonconformities with defined escalation paths and review mechanisms.

5.1.1.4 Documentation Management and Communication Structures

The organisation maintains robust and systematically governed processes for the management of documented information and for internal and external communication, both of which constitute important support requirements under ISO 28000. The Manage Information process (HOW-0089) applies uniformly to all documented information across the organisation, establishing formal requirements for identification, version control, access management and retention. The Manage Communication guidelines (INF-0620) provide a structured framework for both internal and external communication based on the RAPID method, specifying with whom communication should occur, when and how. The structured quarterly management review cycle, governed by the Annual Planning Wheel (GMS-0275), further ensures that documented outputs from performance evaluation are systematically produced and retained.

These processes directly address the requirements of the clause on support, which requires organisations to determine and control internal and external communications relevant to the security management system and to ensure that documented information is available, protected and properly managed. Nunhes et al. (2019) present process standardisation and systemic alignment as central to successful management system implementation and the uniformity and formal governance of the organisation's documentation and communication processes reflect this principle. Domingues et al. (2016) argue that integrated management systems enhance organisational coherence by aligning processes and reducing fragmentation between departments, suggesting that the existing documentation infrastructure provides a strong foundation that could be extended to encompass supply chain security without requiring the construction of an entirely new system.

5.1.1.5 Supplier Contractual Requirements as Operational Governance

The Security Annex and the SCoC together constitute a formally structured contractual instrument through which security obligations are communicated to and imposed on the supplier network. The Security Annex is applied proportionally, calibrated to each

supplier's exposure across the three dimensions of confidentiality, integrity and accessibility, while the SCoC applies universally across all supplier contracts. This proportionality principle reflects the risk based governance logic that ISO 28000 prescribes and aligns with the argument that security requirements should reflect actual vulnerability rather than being applied uniformly across all supplier relationships (Williams et al., 2008).

These instruments reflect the requirements of the clause on operation by establishing a formal basis for extending security governance beyond the company's organisational boundaries to encompass upstream supply chain actors. Fonseca et al. (2017) argue that formalised management systems serve as governance infrastructures that institutionalise structured processes and the contractual framework provides a meaningful foundation consistent with this logic. The proportional application of the Security Annex further demonstrates that the organisation has developed a degree of differentiation in how security obligations are assigned, which aligns with the risk based approach to supplier management that the standard prescribes.

Institutionalisation requires that instruments are not only presented but actively understood and applied. Interview data indicates that suppliers at times sign the Security Annex without adequately understanding the content of the requirements set out in it, generating a divergence between the documented security level and the actual security level within the supplier network. To achieve full alignment with ISO 28000, the Security Annex and SCoC would need to be supported by structured onboarding and verification mechanisms ensuring suppliers genuinely understand and could demonstrate compliance with the requirements set out in it, rather than functioning primarily as contractual formalities.

While the Security Annex and the SCoC satisfy the structural requirements of the clause on operation, the governance logic of ISO 28000 does not treat the existence of contractual commitments as equivalent to the management of security risk. The standard requires that controls are effective, that compliance is verifiable and that the organisation maintains reliable evidence of supplier adherence to its security requirements. None of these conditions are currently met in a systematic manner. The problem is not that suppliers fail to sign the Security Annex. It is that signing the Security Annex and complying with it are not equivalent and the organisation currently has no structured mechanism to distinguish between the two. Respondent 10 characterises this as the most dangerous scenario within the supplier network, because it produces an illusion of control rather than genuine risk mitigation. From a security governance perspective, a supplier that has signed a requirement without adequately understanding it may be more problematic than a supplier whose noncompliance is known and actively managed.

Żurawski et al. (2025) argue that security effectiveness depends on the institutionalisation of verification procedures rather than on the formal existence of requirements and Wieland and Wallenburg (2013) identify the gap between contractual commitment and operational practice as a fundamental challenge in supply chain security governance. The clause on performance evaluation requires that the organisation monitors and measures security management system performance, including supplier compliance and maintains documented evidence of results. Without a verification mechanism, this requirement cannot be met. Achieving conformance would require the establishment of a structured supplier compliance verification process with defined criteria, frequencies, responsible parties and documented outcomes, providing the organisation with reliable and auditable evidence of whether contractual security commitments are being met in practice.

5.1.2 Areas of Partial Alignment

Partial alignment, as applied in this analysis, refers to organisational areas where structures, instruments or initiatives exist that meaningfully address requirements of ISO 28000, but where the scope, consistency, formalisation or institutional embeddedness of these efforts falls short of what the standard requires. These are not areas of absence, but rather areas of incomplete development, where existing practices reflect genuine organisational intent and provide a tangible foundation for further progress. The distinction from areas of substantial alignment lies in the degree to which these practices are systematically applied, formally governed and sufficiently broad in their coverage to meet the standard's requirements across the organisation as a whole. Understanding these areas is analytically important, as they represent the most immediate opportunities for targeted development and the organisational capabilities upon which a more comprehensive supply chain security management system could be built.

5.1.2.1 Scope Definition and Context Analysis

The organisation's decentralised approach, in which each functional area or unit determines its own scope, reflects a pragmatic response to genuine operational heterogeneity and is not without theoretical support, as Jüttner et al. (2003) acknowledge that risk exposure varies significantly across supply chain tiers and organisational interfaces. The tools to support context analysis, including Understanding the Organisation and its Context (INF-1223) and Interested Parties Analysis (INF-0646) , exist and are formally available. The Security Legal Analysis (CZ-2020-182) is also established, while local legal requirements are managed through the Security Operations Manual for Group (INF-0506).

The clause on organisational context, requires organisations to establish a defined scope for the security management system, grounded in a systematic analysis of the internal and external context in which the organisation operates, including the needs and expectations of interested parties relevant to supply chain security. The absence of a

corporate level scope boundary for supply chain security means that cross organisational consistency cannot be assured, that comparable assessments across functional areas cannot be made and that the documented scope requirement of the standard is only partially fulfilled. The context analysis tools are structured primarily in relation to ISO 27001 rather than ISO 28000, limiting their applicability to supply chain security specifically. Domingues et al. (2016) argue that scope fragmentation across organisational units undermines systemic coherence, a concern directly reflected in the variation of supply chain security maturity observed across the functional areas. To achieve full alignment, a structured scoping exercise would need to be conducted at the relevant organisational level, resulting in documented decisions regarding the boundaries, applicability and purpose of the supply chain security management system, explicitly informed by the supply chain security context rather than transposed from the existing ISO 27001 infrastructure.

5.1.2.2 Risk Assessment Coverage and Supplier Classification

A structured risk assessment process exists in the form of the Security Risk Assessment (INF-0513) and the mandatory screening provides a baseline control across all procurement activities. The security risk assessment encompasses five steps covering planning, identification, analysis, management as well as reporting and is intended to be conducted at planned intervals and whenever significant organisational changes occur, demonstrating that the organisation has recognised the need for a structured and proactive approach to security risk management beyond the reactive handling of individual incidents.

This partial alignment becomes evident when examining its application in practice. The clause of planning requires proactive risk assessment covering a broad range of dimensions, including information management, interdependencies between suppliers as well as environmental and cultural factors. Interview data indicates that risk processes beyond the screening are less clearly defined in terms of methods as well as responsibilities and that supply chain security activities are largely driven by requests from procurement personnel rather than by a proactive and systematic approach. This pattern reflects what Jüttner et al. (2003) identify as a risk of fragmented risk perception and inconsistent mitigation efforts across organisational interfaces when structured approaches are absent or inconsistently applied.

Adding to this, the existing supplier classification relies on the Kraljic matrix, which does not incorporate security specific dimensions such as information exposure or strategic dependency. Tummala and Schoenherr (2011) emphasise that effective risk management requires consistent evaluation criteria applied across all supplier relationships, enabling prioritisation based on comparable exposure assessments, a condition that the current approach only partially satisfies. To achieve full alignment, the security risk assessment process would need to be explicitly adapted to address supply chain security as a distinct risk domain. Ongoing efforts to introduce a

classification of HSBI suppliers aim to differentiate suppliers based on scope to determine which security requirements apply, with supporting instructions being developed and requirements to be imposed on procurement. A supplier classification structure explicitly designed for supply chain security purposes would nonetheless still need to be established with defined criteria, documented decision rules and a structured review mechanism to achieve full maturity.

5.1.2.3 Security Governance Does Not Extend to Supply Chain Domain

The company maintains a well defined governance structure for security, with roles and responsibilities formally distributed through the RAPID method in Security Operations Manual for Group (INF-0506) and Security Positions, Roles and Organisation (INF-0512). The Sourcing Council structure further demonstrates that functional governance mechanisms exist and are operational. These structures reflect organisational investment in security governance and provide a basis that partially addresses the requirements of the clause on leadership and support. However, security and supply chain security are distinct functional domains within the organisation and the formal role structure that governs the former does not extend to the supply chain security in all equivalent manner. The RAPID based role definitions and the governance frameworks within Security Operations Manual for Group (INF-0506) and Security Positions, Roles and Organisation (INF-0512) are structured around the broader security management system aligned with ISO 27001 and do not formally assign supply chain security specific responsibilities as a distinct governance domain. Supply chain security capacity typically consists of a limited number of individuals, which does not constitute a formal role structure in the institutional sense. It represents a personnel allocation, one that is inherently person dependent and provides no structural guarantee of continuity, coverage or consistent decision making authority throughout the organisation.

The clause on leadership and support requires that responsibilities and authorities within the security management system are formally assigned, documented as well as communicated and that the governance structure provides sufficient capacity to ensure that the system functions as intended. Christopher and Peck (2004) identify clearly defined roles and structured coordination as prerequisites for effective supply chain security governance.

5.1.2.4 Management Review and Performance Evaluation

The Management Review process (HOW-0018), conducted at minimum twice a year at group functions level and structured around the Security Annual Wheel (GMS-0534), provides a functioning governance mechanism that incorporates inputs from security audits, incident reports, risk status and the evaluation of security objectives and produces decisions regarding the annual security plan approved by top management. This structure reflects the kind of systematic and recurring leadership engagement with

security management performance that Domingues et al. (2016) associate with organisational maturity in integrated management systems.

The partial alignment lies in that the management review currently covers supply chain security as part of the broader security management system rather than as a distinct area of evaluation with its own defined inputs, metrics and improvement decisions. The clause on performance evaluation requires that monitoring and measurement cover the specific domains of the security management system and that results are analysed and evaluated systematically. There are no dedicated performance indicators for supply chain security and the objectives established through the annual planning cycle do not disaggregate supply chain security performance. Nunhes et al. (2019) present measurable objective setting and systematic performance evaluation as fundamental to management system maturity, suggesting that the management review's effectiveness as a supply chain security governance mechanism depends on whether supply chain security is explicitly integrated into its scope, inputs and outputs. Thus, to achieve full alignment, the management review process would need to be extended to include supply chain security specific performance data, defined objectives and targeted improvement decisions, ensuring that leadership engagement translates into systematic and documented progress within this specific domain.

5.1.2.5 Awareness, Competence and Supplier Engagement Activities

The *Security Awareness Programme* (INF-0605) and the onboarding process provide an organisational foundation for security awareness, supported by *Communication Guidelines* (INF-0620) and the *Manage Information* process (HOW-0089). Educational security controls at supplier premises and joint visits by security and procurement personnel demonstrate active efforts to strengthen supply chain security awareness externally.

The partial alignment lies in the inconsistency and resource dependency of these activities across the organisation. The clause on support requires demonstrated competence supported by documented evidence, a requirement that current practices do not systematically meet. Educational controls are primarily directed at HSBI suppliers, which from a security perspective is where such efforts are most necessary. However, these activities are largely dependent on the initiative and availability of individual supply chain security personnel rather than governed by a defined programme with allocated resources. No formal requirements have been specified for supply chain security roles, meaning the organisation cannot systematically identify training needs or evaluate whether personnel possess the knowledge necessary to perform their roles effectively. Żurawski et al. (2025) argue that security effectiveness depends on the institutionalisation of procedures rather than on isolated protective measures and the current approach reflects precisely this tension. To achieve full alignment, supplier education and internal awareness activities would need to be governed by a defined programme with explicit scope, frequency, responsibilities and evaluation mechanisms, ensuring that competence development is treated as a

structured organisational process rather than an ad hoc activity dependent on individual effort and available resources.

5.1.2.6 Internal Audit Programme for Supply Chain Security

The Internal Audit Programme (HOW-0019), the Group Internal Audit Instructions (INF-0641) and the Security Audit and Check-Up Process for Suppliers (INF-0596) demonstrate that audit infrastructure exists and is formally governed. Audit results are included in the management review and findings are tracked through the Handle Operational Findings process (HOW-0031), establishing a connection between operational compliance monitoring and governance level oversight. The audit programme is regularly updated to reflect changes in risks, business priorities as well as regulatory requirements and the findings management process incorporates root cause analysis to inform corrective actions.

The clause on performance evaluation requires that the audit programme reflect the importance of processes and the results of previous audits and that supplier audits are conducted systematically at planned intervals rather than driven by resource availability. Tummala and Schoenherr (2011) argue that effective risk management requires consistent methodologies applied at structured intervals to enable prioritisation based on comparable exposure assessments. The current approach, in which audits are conducted primarily in connection with contract events rather than as part of a proactive, risk based programme, satisfies the formal existence requirement of the clause but not its substantive intent. Follow up activities are primarily oriented towards quality rather than security compliance, meaning that the existing supplier monitoring infrastructure does not systematically capture security relevant information. To achieve full alignment, the audit programme would need to be explicitly extended to cover supply chain security as a governed area, with defined criteria, frequencies and responsibilities for supplier directed audit activities, ensuring that audit coverage is proportionate to assessed risk rather than constrained by available resources.

5.1.3 Areas of Significant Nonconformance

Areas of significant nonconformance, as applied in this analysis, refer to domains where the requirements of ISO 28000 are either entirely absent from the company's current organisational practices or where existing structures are misaligned with the standard's requirements that incremental development would be insufficient to achieve conformance. These are not areas where existing efforts fall short of their intended scope, but rather areas where the governance logic, systematic processes or institutional structures required by the standard do not currently exist within the supply chain security domain in any meaningful form. The identification of these areas is analytically significant because it delineates the boundaries of what could be achieved through targeted improvement of existing practices and what would require the deliberate construction of new governance infrastructure. The nonconformances identified below are not primarily resource or maturity problems. These reflect structural design choices

or the absence of such choices, that prevent the organisation from operating in accordance with ISO 28000 regardless of the effort invested at an operational level.

5.1.3.1 Fragmented Ownership of Compliance Across Organsational Functions

One of the most analytically significant structural deficits identified in the empirical material is that responsibility for supply chain security compliance is not clearly defined or formally assigned. Responsibility for supply chain security is currently distributed across several organisational functions without clear coordinating authority, the purchasing officer manages the supplier relationship, the security function is responsible for the requirements, the risk team manages the screening process and supply chain security personnel provide advisory support. No function currently holds responsibility for supplier compliance over time, including the ongoing verification that security commitments made at contract signature are maintained, updated and enforced as the supplier relationship evolves.

This fragmentation is not a consequence of insufficient resources or individual negligence. It is a structural design problem. The clause on leadership and support requires that roles, responsibilities and authorities within the security management system are formally assigned, documented as well as communicated and that accountability for security outcomes is traceable to defined organisational positions. As Respondent 13 notes, the responsibility for following up on supplier compliance with the Security Annex is unclear, with persistent uncertainty regarding whether this falls on the purchasing officer, the supply chain security function or another actor. This uncertainty means that compliance gaps are not systematically identified or escalated, not because no one notices them, but because no one is structurally positioned to act on them.

Wieland and Wallenburg (2013) argue that effective supply chain governance requires coordination mechanisms that are formally embedded within organisational structures rather than dependent on informal negotiation between functions. Where ownership of compliance is distributed without a coordinating authority, the result is that each function fulfils its own mandate without any single actor holding responsibility for the integrity of the whole. Christopher and Peck (2004) identify this kind of structural accountability gap as a fundamental barrier to supply chain resilience, because disruptions that span functional boundaries, as supply chain security incidents typically do, cannot be governed by any single function acting in isolation. Addressing this nonconformance would require a formal governance decision designating a responsible function or role with explicit authority over supplier compliance monitoring across the full lifecycle of the supplier relationship, supported by defined processes for how compliance information is collected, reviewed and acted upon across functional boundaries.

5.1.3.2 Informal Coordination as a Substitute for Formal Governance

The SME group currently fulfils a coordination function for the supply chain security operations. It connects supply chain security personnel across the functional areas, establishes shared procedures and functions as the primary forum through which common approaches to supply chain security challenges are formulated. This function is valuable precisely because no formal governance structure currently performs it. The SME group therefore does not complement formal governance but instead compensates for its absence.

This distinction is important because the clause on leadership and support requires that the governance of the security management system be grounded in formally defined roles with documented mandates, sufficient resources and institutional authority. An informal group whose outputs carry no formal authority and whose continuity depends on the engagement of its individual members does not satisfy these requirements, regardless of its operational effectiveness. Wieland and Wallenburg (2013) emphasise that relational competencies and coordination mechanisms must be embedded within formal governance structures to be sustainable and consistent. The SME group, as currently constituted, is susceptible to both individual dependency and broader organisational change, whereby departures, reprioritisation or resource constraints could materially undermine its function in the absence of any formal safeguard or remedial mechanism.

The deeper problem is that the absence of formally defined supply chain security roles means that decision making authority within the domain is not institutionally grounded. Decisions regarding supplier classification, the application of the Security Annex, the escalation of compliance concerns and the prioritisation of oversight activities are made through informal channels and individual judgement rather than through defined processes with traceable accountability. This is inconsistent with the systematic decision making logic that ISO 28000 requires and that Fonseca et al. (2017) identify as a prerequisite for effective management system governance. Achieving conformance on this dimension would require the formalisation of supply chain security roles at relevant organisational levels, with documented mandates, defined decision making authorities and sufficient institutional resources to ensure that the coordination function currently performed informally is sustained through governance structure rather than individual commitment.

5.1.3.3 Security Performance Lacks a Defined Measurement Structure

The clause on planning and performance evaluation requires organisations to establish documented security objectives at relevant functions and levels, ensuring that these objectives are measurable, monitored and communicated and to determine what needs to be measured and evaluated in relation to the performance and effectiveness of the security management system. No supply chain security specific objectives or key performance indicators currently exist within the company's governance structure.

The analytical significance of this nonconformance extends beyond a documentation deficit. The absence of defined objectives prevents the PDCA cycle from functioning coherently for supply chain security, as there is no defined basis against which to evaluate performance or identify improvement needs (Fonseca et al., 2017). The management review process cannot evaluate supply chain security performance in any meaningful way, the internal audit programme cannot assess whether supply chain security activities are achieving their intended results and the organisation cannot demonstrate systematic progress in this domain over time. Ho et al. (2015) emphasise that effective supply chain risk management requires measurable outcomes and systematic evaluation mechanisms that enable organisations to assess whether their risk management activities are achieving their intended results and to adjust those activities in response to performance data.

The absence of supply chain security metrics also means that the organisation has no reliable mechanism for distinguishing between periods of security improvement and periods of apparent stability that may in fact involve accumulating risk. Achieving full conformance would require the establishment of a documented set of supply chain security objectives at relevant organisational levels, complemented by defined measurement methods, responsible parties and evaluation timelines as well as the integration of supply chain security performance data into both the management review process and the internal audit programme.

5.1.3.4 Context Analysis Lacks Adaptation to the Supply Chain Domain

The clause on organisational context requires organisations to systematically determine the external and internal issues relevant to the purpose of the security management system, including those arising from the supply chain context and to monitor and review this information. So while the organisation maintains structured processes for context analysis within its broader management system, these are oriented towards the general security management system aligned with ISO 27001 and do not specifically address the supply chain security context. The contexts in which different functional areas and business units operate differ substantially in terms of customer requirements, regulatory frameworks as well as threat landscapes and the existing context analysis infrastructure does not currently capture supply chain security as a distinct domain requiring its own systematic analysis.

Ghadge et al. (2012) argue that supply chain risk management requires a thorough understanding of the specific context in which supply chain relationships operate, including the geopolitical environment, the regulatory landscape and the threat profiles associated with different supplier categories and geographic regions. Thus, without a systematic context analysis specific to supply chain security, the organisation cannot reliably identify which external developments, such as changes in sanctions regimes, emerging threat actors or new regulatory requirements, are most relevant to its supply

chain security governance, nor can it ensure that the security management system is calibrated to the actual risk environment in which it operates. The absence of a dedicated supply chain security context analysis also means that the organisation's approach to supplier risk assessment, security requirements and governance priorities is not grounded in a systematic and documented understanding of the environment in which supply chain relationships are conducted.

Achieving conformance would not necessarily require the construction of an entirely new context analysis process. The tools and governance mechanisms that currently support context analysis within the broader security management system provide a functional basis that could be extended to encompass the requirements of ISO 28000 alongside those of ISO 27001. What is required is a deliberate and documented extension of the existing process scope, ensuring that supply chain security specific issues are addressed and systematically identified, recorded and reviewed at appropriate intervals. This extension would further need to be formally connected to the risk assessment and planning processes of the security management system, ensuring that the context analysis produces actionable governance outputs rather than functioning as a separate documentation exercise.

5.1.3.5 Accumulated Risk Exposure Falls Outside Current Classification Logic

A nonconformance that is structurally embedded in the current approach to supplier management and that is not expected to be visible through operational monitoring alone, concerns the progressive accumulation of security relevant exposure by suppliers who individually appear to fall below the thresholds that would trigger elevated scrutiny. The existing supplier classification logic, based on the Kraljic matrix, assesses each supplier relationship against commercial and strategic criteria at a fixed point in time. It does not account for the fact that a supplier's aggregate knowledge of the company's operations, sensitive processes or security relevant information may grow substantially over the course of a relationship, even if no single transaction or interaction crosses the threshold for heightened classification.

A supplier engaged in multiple procurement cycles or across multiple functional areas, may accumulate a composite picture of the company's supply chain, operational dependencies and security vulnerabilities that constitutes a material risk exposure, without that exposure ever being formally assessed or classified as such. Group level functions are intended to support classification efforts across all functional areas, providing a means to identify and assess such accumulated exposure at an organisational level. The clause on planning and operation requires that risk assessment is comprehensive and proactive and that controls are tailored to the actual risk profile of supplier relationships rather than to a static classification determined at contract initiation. Tummala and Schoenherr (2011) argue that effective risk management must be dynamic and responsive to changes in the risk environment and Christopher and

Peck (2004) identify the failure to account for dependency accumulation as a structural vulnerability in supply chain governance.

The practical implication is that the organisation's current classification logic produces a systematically incomplete risk picture, suppliers are assessed upon entering the relationship rather than as the relationship evolves and the cumulative dimension of information exposure is not operationalised as a governance trigger. Addressing this nonconformance would require the introduction of a dynamic classification mechanism that reviews supplier risk profiles at defined intervals and in response to changes in the scope or depth of the supplier relationship, with explicit criteria for when accumulated exposure warrants reclassification and elevated oversight.

5.2 Improvement Measures and Their Governance Implications

The improvement measures presented are grounded in the gap analysis findings and reflect the structural conditions identified as necessary for supply chain security to function as a governed domain in its own right. Rather than constituting a comprehensive implementation roadmap, the measures represent a structured set of governance interventions designed to address the most consequential deficiencies identified across the organisation's current supply chain security practices. Each measure responds to a specific structural deficiency and together the measures form an interconnected set of interventions whose collective implementation would establish the governance architecture that a coherent and continuously improving supply chain security management system requires.

5.2.1 Proposed Measures for Improvements

The improvement measures proposed are derived from the gap analysis findings presented and intended to provide guidance for further development of supply chain security management in a consistent and structured manner. The measures are structured in accordance with the gaps identified during the analysis. Priority is assigned to areas of significant nonconformance, as these represent fundamental structural deficiencies that compromise the integrity of the management system as a whole and until such deficiencies are remediated, interventions in other areas cannot be expected to give reliable governance outcomes. Areas of partial alignment are addressed subsequently, given that a proportion of the identified deficiencies may be resolved through targeted enhancement of existing processes rather than the establishment of entirely new ones. Areas of substantial alignment fall outside the scope of the improvement measures set out in this section, as the practices currently in place within those areas are already consistent with the governance principles of a structured security management system and require principally documentation and systemic integration rather than substantive development or revision.

5.2.1.1 Clear Ownership of Supply Chain Security Compliance

A significant structural limitation identified is the absence of a clearly designated function holding responsibility for supply chain security compliance across the full lifecycle of supplier relationships. Responsibility is currently distributed across several organisational functions without a coordinating authority, meaning that no actor is structurally positioned to ensure that security commitments made at contract signature are maintained, verified and enforced as supplier relationships evolve over time. This fragmentation is not a consequence of insufficient individual effort but a structural design problem that produces persistent uncertainty regarding who is responsible for follow up on supplier compliance.

Formally assigning a specific function or role with explicit and documented authority over supply chain security compliance oversight is therefore the most consequential governance action available to the organisation. This designation should be embedded within the existing RAPID structure and specify the function accountable for monitoring compliance across the supplier lifecycle, the mechanisms through which compliance information is collected and reviewed and the channels through which identified noncompliance is escalated. This foundational governance decision is a prerequisite for the effective implementation of all other improvement measures proposed, as its absence leaves individual process improvements vulnerable to the same informal dependencies and functional fragmentation that characterise the current state.

Wieland and Wallenburg (2013) argue that effective supply chain governance requires coordination mechanisms that are formally embedded within organisational structures rather than dependent on informal negotiation between functions and Christopher and Peck (2004) identify structural accountability gaps as fundamental barriers to supply chain resilience precisely because disruptions that that extend beyond functional boundaries cannot be governed by any single function acting in isolation. The designation of a responsible function addresses both concerns by providing the structural basis that supply chain security governance presently lacks.

5.2.1.2 Formalisation of the Supply Chain Security Coordination Function

The SME group currently performs a valuable and practically necessary coordination function across the functional areas, connecting supply chain security personnel, establishing shared working methods and functioning as the primary forum through which common approaches to supply chain security challenges are developed. Its outputs carry no formal authority and its continuity depends entirely on the voluntary engagement of its individual members. The SME group therefore does not complement formal governance but compensates for its absence and this distinction has significant implications for the sustainability of the coordination it provides.

Formalising the SME group's coordination function through a documented mandate that specifies its scope, composition, decision making authority and meeting structure

would address this condition without requiring the creation of new organisational units or a formal committee structure. What is required is that the role the group performs in supply chain security governance is formally recognised within the global management system, ensuring that coordination across functional areas is sustained through governance structure rather than individual commitment. Fonseca et al. (2017) argue that management system maturity is linked to the institutionalisation of structured processes and that the effectiveness of coordination mechanisms depends on whether they are formally embedded within the organisation rather than operating informally alongside it. Formalising the SME group's mandate would directly address this condition while preserving the practical value of an arrangement that already functions well in operational terms.

5.2.1.3 Measurable Objectives for Supply Chain Security

No supply chain security specific objectives or key performance indicators currently exist within the organisation's governance structure. The strategic operating plan (SOP) produced by the SME group establishes shared goals and activities for the coming year and represents a starting point for more formalised objective setting, yet it does not currently constitute a governed performance management structure in which objectives are measurable, formally approved or systematically evaluated. The PDCA cycle cannot operate coherently in relation to supply chain security in the absence of such a structure, as no defined basis exists against which performance may be evaluated or needs for improvement identified.

Security challenges become visible primarily through adverse events, which makes proactive objective setting particularly consequential. In the absence of defined targets, a lack of visible incidents may be misread as evidence of effective risk management, when undetected risk may in fact be accumulating. Structured objectives therefore provide a systematic basis for evaluating whether risk management activities are producing their intended effects, rather than treating incident absence as an indicator for security performance. A defined set of supply chain security objectives should therefore be established at a relevant organisational level, complemented by associated measurement indicators. These objectives need not be numerous or technically complex. A practical approach would be to differentiate the acceptable risk threshold by supplier category, where standard suppliers may be assessed against a defined set of requirements through a structured evaluation form, while HSBI suppliers are subject to significantly stricter criteria and more frequent assessment with a considerably lower tolerance for identified deviations. This differentiation makes the objective structures both operationally manageable and risk proportionate. These objectives should be integrated into the existing annual planning cycle, formally approved through the management review process and embedded within the SOP as a governed component of the supply chain security function's yearly activities.

Ho et al. (2015) emphasise that effective supply chain risk management requires measurable outcomes and systematic evaluation mechanisms that enable organisations to assess whether their risk management activities do achieve their intended results. Domingues et al. (2016) similarly associate the definition of domain specific performance indicators with organisational maturity in integrated management systems, suggesting that the absence of supply chain security metrics represents not only a compliance gap but a broader maturity constraint that limits the organisation's ability to develop systematically over time.

5.2.1.4 Integration of Supply Chain Security into Risk Assessment

A structured risk assessment process exists though the Security Risk Assessment (INF-0513) and the mandatory screening procedure, both of which provide a baseline for security risk management across procurement activities. Processes for risk management beyond the screening are less clearly defined in terms of methodologies and responsibilities, while the existing supplier classification relies on the Kraljic matrix, which does not incorporate security specific dimensions.

The Security Risk Assessment process (INF-0513) should be formally extended to explicitly address supply chain security as a defined risk domain. The five step structure of the existing process is suitable for this purpose and does not necessitate redesign. The assessment methodology should therefore include documented supply chain security specific risk criteria covering information exposure, supplier ownership structures, geographic concentration and strategic dependency. The HSBI classification should be formally integrated into the process as a structured risk category, supported by explicit and documented criteria that enable consistent application across functional areas and initiate defined governance responses within the risk assessment process itself. This integration ensures that the HSBI classification serves as an established input to the assessment, monitoring and escalation of security risk across the organisation, rather than functioning solely as a procurement label.

The issue of accumulated risk exposure needs particular attention in this regard. A supplier that has access to limited but recurring information over an extended period may gradually accumulate a composite overview of the company's operations, dependencies and security vulnerabilities, while still remaining below the thresholds applied in the current classification logic. Tummala and Schoenherr (2011) argue that effective risk management must be dynamic and responsive to changes in the risk environment rather than based on static assessments conducted at contract initiation and Hallikas et al. (2004) note that cumulative exposure is difficult to identify without structured criteria and defined review intervals. Addressing this requires a dynamic review mechanism through which supplier risk profiles are reassessed at defined intervals and in response to changes in the scope or depth of a supplier relationship.

5.2.1.5 A Structured Process for Supplier Compliance Verification

The Security Annex and the SCoC constitute a formally structured contractual basis through which security obligations are communicated to and imposed on the supplier network. The proportional application of requirements relative to each supplier's exposure across the three security dimensions illustrated in Figure 5 is consistent with coherent risk based governance principles. The existence of contractual obligations does not in itself constitute the management of security risk, as the signing of the Security Annex and compliance with its requirements are fundamentally distinct conditions and the organisation currently lacks a structured mechanism to differentiate between the two.

A structured supplier compliance verification process should therefore be established, specifying the assessment methodology, accountable parties and frequency of compliance verification with respect to the Security Annex. The establishment of a defined assessment methodology, applied at relevant intervals throughout the supplier relationship, including at contract renewal, significant scope changes, or periodic review intervals especially for HSBI suppliers, would represent a substantive improvement over the current approach. The results of such assessments should be documented and the function holding responsibility for compliance oversight should have authority to escalate identified noncompliance through defined channels. The existing infrastructure for educational security controls at supplier premises and the audit program for supplier directed activities provide a practical foundation upon which a more systematic verification process could be built without requiring the construction of an entirely new governance structure.

Żurawski et al. (2025) argue that security effectiveness depends on the institutionalisation of verification procedures rather than on the formal existence of requirements and Williams et al. (2008) emphasise that security management requires integration across organisational functions and active coordination with supply chain partners. A supplier compliance verification process addresses both of these conditions by transforming contractual commitments into actively monitored governance obligations.

5.2.1.6 Extension of Context Analysis to Supply Chain Security

The existing tools for context and stakeholder analysis, including Understanding the Organisation and its Context (INF-1223) and the Interested Parties Analysis (INF-0646), are formally established and structurally coherent, yet remain oriented towards the broader security management system in alignment with ISO 27001. They do not address the supply chain security context as a distinct domain, meaning that the environmental, geopolitical and relational factors most relevant to supply chain security are not systematically identified or documented as a basis for governance decisions.

The issue may be addressed through the expansion of the existing templates for context analysis to include supply chain security as a defined category of analysis, without necessitating the establishment of a separate process. A specific section of the existing template should identify the internal and external factors most relevant to supply chain security. The results of the analysis should be formally connected to the risk assessment process through the Security Risk Assessment (INF-0513), ensuring that the context analysis supports effective governance outcomes rather than functioning merely as a separate documentation requirement. The addition should further be connected to the Interested Parties Analysis (INF-0646) to ensure that stakeholders with particular relevance to supply chain security, including key suppliers, customers with security requirements and relevant regulatory authorities, are identified and their needs assessed within the existing stakeholder framework.

Ghadge et al. (2012) argue that supply chain risk management requires a thorough understanding of the specific context in which supply chain relationships operate, encompassing geopolitical, regulatory as well as relational dimensions and that this understanding must be systematically produced and documented rather than assumed. In the absence of a context analysis that explicitly addresses the supply chain security environment, the organisation cannot reliably identify which external developments are most pertinent to its governance priorities, nor ensure that its risk assessment processes are responsive to the actual threat environment in which it operates.

5.2.1.7 A Structured Programme for Awareness and Competence Development

Supply chain security personnel currently provide training and education to procurement personnel on security requirements, yet this takes place on a non systematic basis rather than as part of a governed programme. Educational controls at suppliers premises are similarly driven by individual initiatives and available resources. The level of understanding among procurement personnel consequently varies considerably and suppliers may sign the Security Annex without adequately understanding the content of the requirements, a concern that illustrates the gap between the formal communication of security obligations and their practical understanding within the supplier network.

A defined supply chain security awareness programme should be established with HSBI suppliers and procurement personnel as its primary target groups, given that these represent the highest risk interfaces within the supply chain. The programme should specify the expected frequency of training activities directed at procurement personnel, the criteria for prioritising which suppliers receive educational controls and the methodologies of documenting completion across both internal and external activities. Formal competence requirements for supply chain security roles should be described sufficiently to enable the identification of training needs and the evaluation of whether personnel possess the knowledge necessary for their responsibilities. The existing Security Awareness Programme (INF-0605) provides a structural reference point for

the organisation and maintenance of such a programme and an extension of its scope to include supply chain security as a distinct content area for procurement personnel would constitute a practically feasible and substantive improvement. Nunhes et al. (2019) presents process standardisation and systemic alignment as central conditions for successful management system implementation, while the consistency with which awareness activities are applied across the organisation depends on their incorporation into a governed programme rather than their reliance on individual initiative and available resources.

5.2.1.8 Inclusion of Supply Chain Security in Management Review

The management review process constitutes a functioning governance mechanism that incorporates inputs from security audits, incident reports, risk status and the evaluation of security objectives as well as produces decisions regarding the annual security plan approved by top management. Supply chain security is currently addressed as part of the broader security management system rather than as a distinct area of evaluation with its own defined inputs, metrics and improvement decisions, meaning that the management review does not provide the domain specific governance outputs that supply chain security management system requires.

Extending the management review to include supply chain security specific performance data among its structured inputs and to produce documented decisions for improvements, would address the gap within the Security Annual Wheel (GMS-0534) without requiring a separate review process. Domingues et al. (2016) argue that the effectiveness of management reviews in integrated management systems depends on the extent to which domain specific performance data is systematically incorporated as structured input and associate this practice with organisational maturity in governance and continuous improvement. Once supply chain security objectives and measurement indicators have been defined, the management review provides the mechanism through which progress is assessed and acted upon. The Handle Operational Findings process (HOW-0031) already provides the infrastructure for tracking findings to closure with root cause analysis and should be applied explicitly to supply chain security related findings identified through audits, incidents and compliance assessments, ensuring that the management review has access to structured and systematic performance data.

5.2.2 The Proposed Measures in Relation to ISO 28000

The improvement measures proposed are not independently motivated recommendations but constitute a structurally coherent response to the specific requirements of ISO 28000. The measures address the governance conditions that the standard presupposes and that the gap analysis has demonstrated to be absent or insufficiently developed within the current supply chain security function. Each measure corresponds directly to one or more clause requirements of the standard and their collective implementation would move the organisation from a state of partial and

fragmented alignment to one in which a management system capable of supporting certification could be meaningfully established.

The measures address the full clause structure of ISO 28000 and should therefore be understood as a system of interdependent interventions rather than a set of discrete improvements. The sequence in which the measures are presented reflects a deliberate prioritisation logic in which structural governance prerequisites are established before process level refinements are pursued. This sequencing is analytically significant because several of the measures are conditionally dependent on others. Measurable objectives cannot be meaningfully evaluated without a governance structure accountable for their oversight and compliance verification cannot be systematically pursued without a designated function holding authority over its outcomes. The measures should therefore be understood not only in relation to their individual clause requirements, but as constituent elements of the governance architecture that their combined implementation would establish.

The formalisation of compliance ownership and the supply chain security coordination function addresses the requirements of the clause on leadership and support, which requires that roles, responsibilities and authorities within the security management system are formally assigned, documented and communicated. The current distribution of responsibility across multiple functions without a designated coordinating authority prevents the organisation from meeting these requirements regardless of the quality of individual operational efforts. Formally assigning a function with explicit authority over supplier compliance monitoring and embedding the SME group's coordination role within a documented governance mandate, would establish the institutional accountability structure that this clause requires and upon which all other governance mechanisms depend. Christopher and Peck (2004) identify clearly defined roles and structured coordination as prerequisites for effective supply chain security governance and the absence of both within the current supply chain security function is precisely what this measure is designed to address.

The establishment of measurable supply chain security objectives responds directly to the clause on planning, which requires organisations to define security objectives at relevant functions and levels, ensuring that measurable objectives are monitored and integrated into the planning cycle. The measure equally addresses the clause on performance evaluation, which requires that the organisation determines what needs to be measured in relation to the effectiveness of the security management system and that results are systematically analysed and evaluated. Thus, without defined objectives and associated indicators, neither clause would be satisfied in any meaningful sense, as the organisation possesses no defined basis against which to assess whether supply chain security activities are producing their intended outcomes. Domingues et al. (2016) associate the definition of domain specific performance indicators with organisational maturity in integrated management systems, suggesting that the absence of supply chain

security metrics represents not only a compliance gap but a broader maturity constraint that limits the organisation's capacity to develop systematically over time.

The integration of supply chain security into the risk assessment process and the introduction of a dynamic supplier classification mechanism responds to the clause on planning, which requires a systematic and risk based approach to identifying, analysing and evaluating security threats, including those arising from supplier relationships. The current reliance on the Kraljic matrix, which does not incorporate security specific dimensions and the absence of a mechanism for capturing accumulated risk exposure over time, mean that the organisation's risk assessment approach does not satisfy the clause's requirement for comprehensive and proactive risk governance. Tummala and Schoenherr (2011) argue that effective risk management must be dynamic and responsive to changes in the risk environment rather than based on static assessments conducted at contract initiation and extending the security risk assessment process to address supply chain security as a distinct domain with structured reclassification criteria would bring the relevant processes into substantive alignment with both this requirement and that argument.

The establishment of a structured supplier compliance verification process addresses the clause on operation, which requires that the organisation plans, implements and controls the processes necessary to manage identified security risks, including those associated with suppliers and external parties. The clause does not treat the existence of contractual requirements as equivalent to the management of security risk. Rather, the clause requires that controls are applied, that compliance is verifiable and that documented evidence of results is maintained. Tummala and Schoenherr (2011) argue that effective risk management must be dynamic and responsive to changes in the risk environment rather than based on static assessments conducted at contract initiation and extending the security risk assessment process to address supply chain security as a distinct domain with structured reclassification criteria would bring the relevant processes into substantive alignment with both this requirement and that argument.

The extension of context analysis to the supply chain security domain addresses the clause on organisational context, which requires the organisation to systematically determine the internal and external factors relevant to the purpose of the security management system and to monitor and review this information at defined intervals. The current context analysis infrastructure is oriented towards ISO 27001 and does not address supply chain security as a distinct domain. Ghadge et al. (2012) argue that supply chain risk management requires a thorough understanding of the specific geopolitical, regulatory and relational context in which supplier relationships operate and extending the existing templates to capture supply chain specific contextual factors and connecting the outputs formally to the risk assessment process would satisfy this requirement without necessitating the construction of an entirely new process.

The formalisation of the competence and awareness programme responds to the clause on support, which requires that personnel are competent on the basis of appropriate education, training or experience, that the organisation takes action to acquire the necessary competence and evaluates the effectiveness of such actions and that documented evidence of competence is maintained. The current awareness activities, while valuable, are not governed by a defined programme and do not produce the documented evidence of competence that this clause requires. Nunhes et al. (2019) present process standardisation and systemic alignment as central conditions for successful management system implementation and a programme with specified scope, frequency, target groups and evaluation mechanisms would address this condition directly, ensuring that competence development is treated as a governed organisational process rather than an activity contingent on individual initiative and available resources.

The inclusion of supply chain security as a distinct area within the management review process addresses the clause on performance evaluation, which requires that top management reviews the security management system at planned intervals and that the review incorporates defined inputs, including monitoring and measurement results, audit findings and the status of security objectives. The measure additionally addresses the clause on improvement, as the management review constitutes the primary governance mechanism through which nonconformities are identified and corrective actions are initiated at a strategic level. The management review as currently structured does not include supply chain security specific inputs or produce governance decisions directed at this domain. Domingues et al. (2016) argue that the effectiveness of management reviews in integrated management systems depends on the extent to which domain specific performance data is systematically incorporated as structured input and extending the scope of the review to incorporate supply chain security performance data and targeted improvement decisions would ensure that leadership engagement translates into systematic and documented progress, satisfying both the letter and the governance intent of the relevant clauses.

Considered across all proposed measures, the full clause structure of ISO 28000 is addressed in a manner proportionate to the gaps identified in the analysis. The implementation of the measures would not merely bring individual processes into closer alignment with specific requirements but would establish the governing architecture through which a coherent, accessible and continuously improving supply chain security management system could be maintained over time. Fonseca et al. (2017) argue that management system maturity is linked to the institutionalisation of structured processes and the embedding of recurring evaluation and feedback mechanisms within organisational practice and this structure reflects that logic, ensuring that planning, execution, performance evaluation and improvement are systematically interconnected rather than pursued as isolated organisational activities.

5.3 Addressing the Research Questions

The three research questions guiding the investigation have been addressed progressively throughout the analysis. The first concerns how implementing ISO 28000 would influence the organisation's supply chain security practices. The second examines how current practices correspond to the requirements of the standard. The third identifies specific gaps across organisational processes and supplier interfaces. Considered together, the questions form a structured progression from the theoretical implications of the standard to an overall assessment of alignment and a detailed identification of areas requiring development. The responses synthesise the findings presented across the empirical data, gap analysis and improvement measures into explicit answers to each question.

5.3.1 The Influence of ISO 28000 on Supply Chain Security Practices

Implementing ISO 28000 would require the organisation to formalise supply chain security as a distinct governance domain, structurally separate from the broader security management system currently aligned with ISO 27001. The standard requires documented scope boundaries grounded in a systematic analysis of the supply chain security context, a security policy that explicitly addresses supply chain security as a governed area and formally assigned roles with institutional authority and documented decision making mandates. These requirements would not merely add procedural obligations to existing structures but would reframe how supply chain security is positioned within the organisation's governance architecture.

A particularly consequential implication concerns the standard's embedded PDCA logic, which connects planning, operational execution, performance evaluation and continuous improvement into a coherent and recurring governance cycle. For this cycle to function coherently in relation to supply chain security, the organisation would need to establish measurable objectives at relevant organisational levels, integrate supply chain security performance data into the management review process and ensure that operational experience feeds systematically into governance decisions. This would structurally transform the supply chain security function from one that responds to demands as they arise into one that exercises deliberate oversight of its own development over time, which Fonseca et al. (2017) identify as a defining characteristic of management system maturity.

ISO 28000 would further require that supplier compliance is actively verified rather than contractually assumed. The standard does not treat the existence of contractual security requirements as equivalent to the management of security risk. Rather, it requires that controls are applied, that compliance is verifiable and that documented evidence of results is maintained throughout the supplier relationship. This would necessitate structured verification mechanisms with defined criteria, frequencies and accountable parties, fundamentally changing the relationship between the organisation and its supplier network from one of requirement communication to one of ongoing

compliance governance, consistent with the argument that security management requires active integration across organisational functions and coordination with supply chain partners rather than isolated protective measures (Williams et al., 2008).

The standard would also require that risk assessment is comprehensive, proactive and dynamic. This means addressing not only the risk dimensions captured by the current screening process but also physical vulnerabilities, information security threats, supplier interdependencies and the progressive accumulation of exposure over the course of supplier relationships. When combined with a requirement for context analysis specifically oriented towards the supply chain security environment, ISO 28000 would provide a continuous and responsive understanding of the threat landscape, which could then be used as a basis for governance decisions rather than as an occasional analytical activity (Ghadge et al., 2012).

5.3.2 Current Practice Correspondence with ISO 28000 Requirements

Current organisational practices demonstrate meaningful alignment with ISO 28000 in several foundational areas. A documented security policy with top management commitment, an established quarterly management review cycle, a systematically governed screening process applied across all procurement activities, an incident management and corrective action infrastructure providing a functional baseline, robust and uniformly governed documentation and communication processes as well as a proportionally applied contractual framework for supplier security obligations collectively represent a governance foundation that is not incidental. These structures reflect a sustained organisational investment in security management and provide a basis upon which a compliant supply chain security management system could be developed without requiring the construction of entirely new systems, which Domingues et al. (2016) associate with the kind of systemic coherence that integrated management system infrastructure enables.

The overall degree of correspondence is, however, partial rather than substantive. The governance structures, risk assessment processes, competence activities and audit programmes that exist across the organisation have been developed primarily in relation to ISO 27001 and do not extend to supply chain security as a distinct domain with its own defined scope, objectives, roles and evaluation mechanisms. The management review, while systematic, addresses supply chain security as a component of the broader security management system rather than as an area requiring dedicated inputs and governance decisions. The internal audit programme covers supplier directed activities but does so primarily in connection with contract events rather than as part of a proactive, risk based programme with defined coverage criteria. Supplier classification relies on the Kraljic matrix, which does not incorporate security specific dimensions and no formally defined competence requirements exist for supply chain security roles.

The overall picture is therefore one of substantial general management system infrastructure that is not yet configured for supply chain security as a governed domain, combined with a set of operational instruments that are well designed in principle but insufficiently institutionalised in practice (Żurawski et al., 2025). The correspondence is strongest where existing processes could be extended to encompass supply chain security requirements and weakest where the structural conditions required by the standard, particularly formal governance authority, measurable objectives and systematic compliance verification, are absent entirely.

5.3.3 Gaps in Organisational Processes and Supplier Interfaces

The most analytically significant gaps identified span both internal governance processes and supplier interfaces, several of which are structurally interconnected in ways that limit the effectiveness of individual process improvements pursued in isolation.

Within internal governance, the most consequential gap concerns the absence of clearly designated compliance ownership across the supplier lifecycle. Responsibility for supply chain security is distributed across several organisational functions without a coordinating authority, meaning that no actor is structurally positioned to ensure that security commitments made at contract signature are monitored, updated and enforced as supplier relationships evolve. This fragmentation is not a consequence of individual negligence but a structural design condition that produces persistent uncertainty regarding accountability and generates compliance gaps that are neither systematically identified nor escalated. Wieland and Wallenburg (2013) argue that effective supply chain governance requires coordination mechanisms that are formally embedded within organisational structures rather than dependent on informal negotiation between functions and the current distribution of responsibility across multiple functions without a designated coordinating authority reflects this condition. Related to this, the coordination currently provided by the SME group is operationally valuable but constitutes an informal substitute for formal governance rather than a complement to it. Its outputs carry no institutional authority and its continuity depends on individual engagement, making the coordination function it performs inherently vulnerable to organisational change (Fonseca et al., 2017).

Risk assessment beyond the mandatory screening process is inconsistently defined in terms of methods and responsibilities and is largely reactive rather than proactive. The existing supplier classification, based on the Kraljic matrix, does not capture security specific dimensions including information exposure, ownership structures or strategic dependency and critically does not account for the gradual accumulation of sensitive knowledge by suppliers across extended relationships. Tummala and Schoenherr (2011) emphasise that effective risk management must be dynamic and responsive to changes in the risk environment rather than based on static assessments conducted at contract initiation and the current classification logic does not satisfy this condition. A

supplier operating within the organisation's environment over time may develop a composite picture of its operations, dependencies and security vulnerabilities without that accumulation ever triggering a governance response under the current classification logic. The absence of supply chain security specific objectives and performance indicators further means that the PDCA cycle cannot operate coherently for this domain, leaving the organisation without a reliable mechanism for distinguishing between genuine security improvement and periods of apparent stability in which risk may in fact be accumulating undetected (Ho et al., 2015).

At supplier interfaces, the primary gap lies between the formal existence of contractual security requirements and their verified application in practice. The *Security Annex* establishes a comprehensive and proportionally applied contractual basis for supplier security obligations, but the signing of the annex and compliance with its requirements are fundamentally distinct conditions and the organisation currently lacks a structured mechanism to differentiate between the two. Żurawski et al. (2025) argue that security effectiveness depends on the institutionalisation of verification procedures rather than on the formal existence of requirements and the current approach reflects precisely this gap. Suppliers may execute the annex without adequately understanding its content and awareness and educational activities directed at the supplier network are conducted on a nonsystematic basis dependent on individual initiative and available resources rather than governed by a defined programme with specified scope, frequency and evaluation criteria. The result is that the contractual governance infrastructure, while well designed, produces an incomplete picture of actual security conditions within the supplier network and the organisation cannot reliably distinguish between documented compliance and operational compliance across its supply chain (Williams et al., 2008).

6. Discussion

The chapter deepens the analysis by examining the gap between the organisation's stated security ambitions and its current structural conditions. It argues for the necessity of an extended framework incorporating a strategic governance layer and a continuous improvement loop that connects operational processes to governance level decisions.

6.1 Foundation and Structural Deficiency

The gap analysis reveals a supply chain security function with a solid organisational foundation, but one whose capacity to achieve its purpose is limited by structural constraints. Although the organisation shows alignment with ISO 28000 in several areas, deeper structural deficiencies remain that extend beyond the scope of incremental operational improvement. These deficiencies do not represent isolated process failures, but rather reflect a broader organisational condition in which the scope and ambition of supply chain security governance have expanded considerably, while the formal structures required to support that governance at a corresponding level of maturity have not developed to the same extent.

Two interconnected themes structure the discussion. The first concerns the resource and institutional conditions that characterise the current state of supply chain security governance and the extent to which those conditions are insufficient to support the level of systematic and continuously improving security management that both ISO 28000 and the organisation's own stated ambitions require. The second addresses the proposed development areas and argues for their necessity as a direct response to the structural gaps identified in the analysis. The central argument is that the proposed measures do not constitute supplementary enhancements to an already functional system, but rather represent the minimum organisational foundation required to transform existing operational practices into a coherent, assessable and continuously improving management system. The individual components cannot be understood in isolation from one another, nor from the institutional conditions that determine whether such a transformation is achievable in practice.

6.2 Strategic Ambition and Structural Insufficiency

Over an extended period, the organisation has developed a well established and mature security function within its own operations. Through structured governance, clearly defined roles and a deeply embedded security culture, the organisation has demonstrated a substantive understanding of what it means to treat security as a core organisational priority and of the institutional investment required to achieve a high level of security maturity. This accumulated experience is not incidental, but reflects a sustained organisational commitment to developing security as a fundamental capability rather than addressing it as a compliance obligation. In this respect, the organisation possesses an established reference point for what effective security

governance requires. The challenge is that supply chain security, as a distinct governance domain, has not yet attained a comparable level of maturity and the conditions currently in place are not sufficient to bring it to that level.

Supply chain security as a distinct organisational function is a comparatively recent development within the company and during its formative phase the resources allocated to it were broadly proportionate to the demands then placed upon it. Its initial area of responsibility was to establish security requirements, integrate security considerations into procurement processes and support awareness across the supplier network. At that stage, an operationally focused function with limited dedicated capacity constituted a reasonable point of departure. The more important issue is whether this original setup has become a permanent part of the organisation and what that means for a company with such broad security ambitions.

A particularly instructive illustration of this condition is the role currently performed by the SME group within the organisation. The group connects supply chain security personnel across functional areas, develops shared working methods and serves as the primary forum through which common approaches to supply chain security challenges are formulated. In practice, it fulfils a coordination and governance function that is both valuable and necessary to the effective operation of supply chain security across the organisation. The difficulty is that it does so on an informal basis, without a documented mandate, without formal decision making authority and with a continuity that is contingent entirely upon the voluntary engagement of its members. The SME group therefore does not complement a formal governance structure. It substitutes for one. That substitution, however effective in the short term, reflects precisely the nature of the structural gap that dedicated resources and formalised arrangements would be required to address. The fact that a group of committed individuals has established a functional approach to coordination in the absence of formal institutional infrastructure is an expression of organisational capability, not a justification for leaving that infrastructure unestablished.

The security policy expresses an ambition to be globally recognised for high security awareness and strong professional capability in risk management. It positions security not as a compliance obligation but as a core organisational capability and a source of both competitive and reputational strength. If that ambition is treated as a substantive organisational commitment rather than a clarification statement, it follows that every domain of security governance, including supply chain security, must attain a level of maturity that is coherent with it. A supply chain security function that remains primarily reactive, operationally constrained and structurally unable to develop systematically over time cannot sustain a globally recognised security posture. The distance between the stated ambition and the current state of the function is therefore not solely a matter of insufficient resources. It constitutes a strategic inconsistency that, if left unaddressed, risks undermining the credibility of the organisation's broader security commitment.

The particular consequence of this condition is determined by the character of security as a discipline. Many organisational capabilities reveal their deficiencies in real time, whereas security does not. Weaknesses accumulate incrementally, risks go undetected and the absence of incidents could easily be mistaken for evidence of effective management. An organisation that lacks the capacity to proactively evaluate its supply chain security posture may therefore remain unaware of its vulnerabilities precisely until the point at which they materialise. In this respect, underinvestment in supply chain security does not constitute a neutral organisational condition. It represents a form of risk accumulation that does not register within existing oversight mechanisms but develops gradually in the absence of the structural capacity required to identify and address it.

The opportunity cost of the current resource situation warrants consideration. Supply chain security personnel with substantive expertise in a complex and strategically sensitive domain are presently directing a considerable proportion of their professional capacity toward individual operational support, guiding procurement personnel through requirements that a more mature governance structure would have embedded systematically across the organisation. That expertise, if applied at a strategic level, could instead be directed toward constructing the governance structures that provide individual support interventions progressively less necessary. It could be employed in developing structured competence programmes that raise the foundational understanding of security requirements across the procurement function as a whole, rather than transferring knowledge through individual interactions. It could be applied to establishing the measurement structures and feedback mechanisms through which the organisation would be able to assess whether its supply chain security efforts are producing their intended outcomes. None of these objectives is achievable at the requisite scale without dedicated organisational capacity and none will be realised through the continuation of existing arrangements alone.

A broader organisational logic is also relevant in this context. The company has already demonstrated that the transition from an emerging security function to a mature and institutionally embedded one is achievable, having completed that transition within its own internal operations. The same investment in governance infrastructure, competence development and systematic improvement that produced the current level of internal security maturity is precisely what supply chain security now requires. The organisation operates in a sector where the security environment is assessed by authorities as increasingly complex and where supply chain dependencies are explicitly identified as strategic vulnerabilities. The expectations placed upon organisations of the company's profile, from customers, regulators and alliance partners, are likely to intensify rather than diminish over time. In that environment, a supply chain security function that is structurally constrained from developing beyond its current state is not maintaining its position. It is losing ground relative to the demands being placed upon

it. The organisations and supply chains that would be best positioned in that environment are those that have invested in governance infrastructure, competence and systematic improvement in advance of the point at which external pressure to do so becomes intense. The commitments expressed in the security policy do not merely permit such an investment but require it.

6.3 A Framework for Coherent Governance

The deficiency within the existing Supply Chain Security Framework is not an absence of processes within its current boundaries, but rather the absence of a governing architecture capable of connecting those processes to one another and to a broader evaluative purpose. An organisation may maintain structured procurement checkpoints, a comprehensive set of security requirements and active screening routines and yet possess no reliable mechanism for determining whether those activities are collectively achieving their intended security outcomes. This constitutes the condition that the extended recommended framework is designed to address and it represents a more fundamental organisational concern than a limited compliance gap. It is a condition in which the organisation is unable to distinguish between the substantive performance of supply chain security management and the procedural appearance of it.

This distinction is of considerable significance because it exposes the existing framework to a specific and insufficiently recognised risk of perceived rather than actual control. When suppliers execute the Security Annex without an adequate understanding of its requirements, the organisation registers a contractual commitment while remaining structurally unable to determine whether that commitment corresponds to operational reality. This does not constitute a marginal or minor risk. It represents a pattern identified in the empirical material, one that has necessitated joint interventions between security and procurement personnel on an individual case basis. A framework that cannot systematically differentiate between the execution of a commitment and compliance with its substantive requirements does not govern security risk. It merely documents the condition and the organisational consequences of the distinction are substantial. The requirement is therefore not for additional documentation, but for a verification mechanism that renders compliance an actively monitored condition rather than a contractual assumption.

The same limitation operates at the level of risk classification. The current Kraljic based classification assigns a risk profile at a fixed point in time and does not revisit it as supplier exposure widens or the external risk environment changes. A supplier operating within the organisation's environment over an extended period may gradually accumulate a depth of insight into its operations, dependencies and security sensitive processes, without that accumulation ever triggering a governance response under the existing logic. The introduction of the HSBI classification acknowledges this problem, but a designation that is not subject to structured periodic review risks becoming a fixed label rather than a living governance instrument. A static classification applied to a

dynamic risk landscape produces a progressively less accurate representation of actual exposure and that inaccuracy is not visible through operational monitoring alone. Dynamic classification and context based evaluation are therefore corrections to a structural design choice that treats supplier risk as stable when it is inherently cumulative, relational and contextually contingent.

At the strategic level, the absence of objectives specific to supply chain security has implications that extend beyond compliance with ISO 28000. Thus, without defined targets, there is no basis for evaluating whether the operational activities are producing security value or merely compliance activity. Incident absence cannot serve as a performance indicator, as it is equally consistent with effective risk management and with undetected risk accumulation. A function without measurable objectives operates in a condition of structural ambiguity about its own effectiveness and that ambiguity cannot be resolved through an intensification of existing activities. It could be resolved only through the establishment of an evaluative framework within which performance may be assessed and improved on a systematic basis. Governance arrangements and leadership engagement specifically dedicated to supply chain security, together with a formalised process for performance evaluation, would transform the function from one that reacts to security demands as they emerge into one that exercises deliberate oversight of its own development over time.

The competence and support dimensions of the extended framework are motivated by a related but distinct gap. Awareness and training activities directed at procurement personnel are conducted within the organisation, both through structured sessions and through individual guidance provided to personnel requiring support in specific procurement situations. The value of these activities in building security competence should not be understated. These are, however, delivered on an irregular basis and are not governed by a defined programme with specified scope, frequency or evaluation mechanisms. Competence development consequently depends on the initiative and availability of individual supply chain security personnel rather than on a structured organisational process, which produces uneven results and does not support the documented evidence of capability that ISO 28000 requires. Formalising the competence programme as a governed component of the supply chain security management system would not introduce an entirely new activity. It would provide the governance structure that existing activities currently lack, ensuring that competence development is treated as a sustained organisational responsibility rather than a supplementary effort contingent on available capacity.

The structural gaps identified across classification logic, compliance verification, strategic governance and competence development share a common characteristic in that they reflect the absence of feedback mechanisms through which operational experience is converted into governance decisions. Risk assessments do not inform classification reviews. Compliance findings do not shape competence priorities.

Incident experience does not feed into the governance cycle in any systematic way. The continuous improvement loop introduced by the extended framework is the structural mechanism that closes these connections and its significance extends beyond any single gap it addresses. Individual processes may be refined in isolation while the systemic condition that produces those gaps remains intact. Once operational experience becomes a structured input to governance decisions, the framework acquires the capacity to develop in response to the security challenges the organisation actually encounters rather than those it anticipated at the point of design. The absence of this loop is therefore not a gap among others. It is the condition that makes the persistence of the others structurally inevitable.

These considerations motivate an extended structure that goes beyond the operational processes currently in place. The recommended extended supply chain security framework, illustrated in Figure 7, introduces a strategic governance layer comprising governance and leadership, objectives and planning, as well as performance evaluation and improvement, positioned above the existing operational processes to provide the governing logic that connects them. At the operational level, dynamic supplier classification, context based evaluation, compliance verification and reclassification triggers address the structural gaps that prevent the existing processes from generating reliable governance outcomes. The support layer specifies the competence programme, communication structures and documented information as formally governed components rather than supplementary activities. A continuous improvement loop connects all layers, ensuring that the experience generated at the operational level reaches governance decisions and that those decisions in turn shape operational activities. The structure is coherent as a whole because none of its components is sufficient alone. The strategic layer without operational refinements would govern processes that remain structurally incomplete. The operational refinements without a strategic layer would generate evidence that no governance mechanism is positioned to act upon.

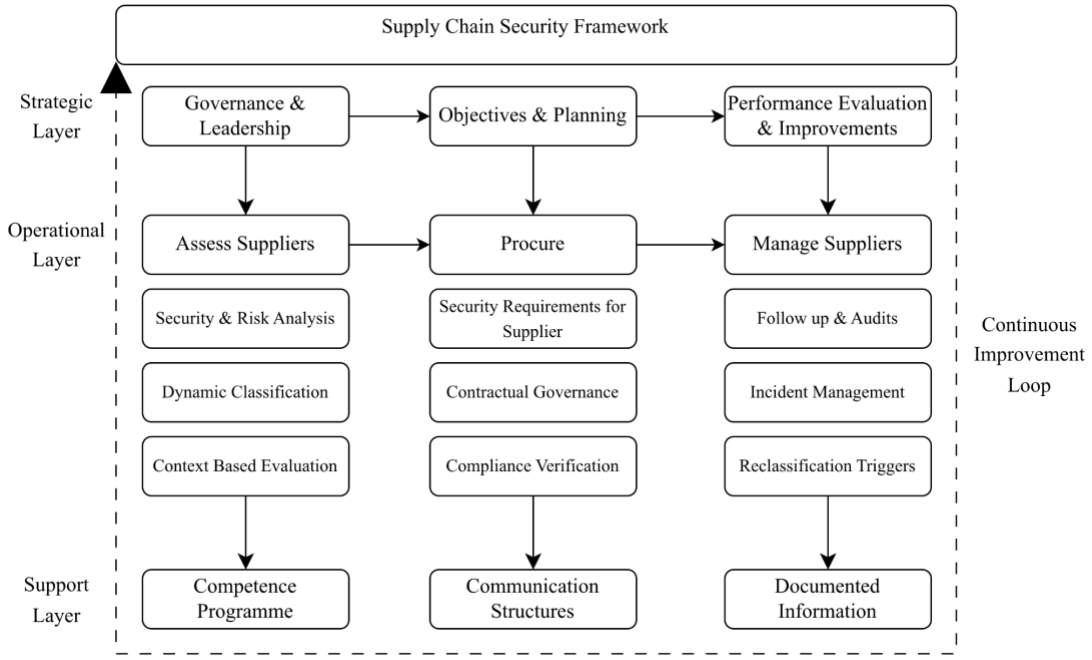

Figure 7. The Recommended Extended Supply Chain Security Framework, depicting the strategic, operational and support levels and the continuous improvement loop connecting them.

7. Conclusions

The chapter summarises the study's principal findings. It concludes that supply chain security needs to be constituted as a governed domain in its own right, with formal compliance ownership, measurable objectives and structured verification mechanisms. The limitations of the analysis and directions for future research are also presented.

7.1 Concluding Observations

Supply chain security has become one of the most important governance challenges for organisations operating in complex and security sensitive environments. The ability to protect not only one's own operations but the entire network of suppliers and partners upon which those operations depend requires a level of structural governance that goes well beyond the establishment of contractual requirements or the application of isolated controls. It is required by an organisation that what is being tried to be achieved is known, that the right people have been designated to pursue it, that the efforts being made could be verified as producing the intended outcomes and that improvements could be made systematically over time. These are not modest demands and meeting them in a sustained and demonstrable manner is what ISO 28000 is designed to ensure.

The analysis reveals an organisation that understands what rigorous security governance entails, that has developed genuine institutional capability within related areas and that has made a substantive start in extending that capability to supply chain security. It equally reveals an organisation that has reached a point at which the distance between its stated ambitions and its current structural arrangements has become consequential and at which the choices made in the period ahead will determine whether supply chain security is governed as the strategic priority that the organisation's own policy declares it to be.

7.2 Structural Conditions and Governance Implications

The organisation examined is not one that has neglected security governance. It is one that has invested in it, sustained it institutionally and developed genuine expertise within it. The challenge is not one of organisational indifference but of institutional design, as the investment made has been directed primarily towards a governance domain that is closely related to, but structurally distinct from, supply chain security and the conditions necessary to govern supply chain security as a domain in its own right have not yet been deliberately established.

The shared high level structure of ISO 28000 and ISO 27001 explains much of the alignment that the gap analysis identifies in foundational areas. The organisation's existing management review cycle, documentation processes, incident management infrastructure and audit programme are all developed within a governance logic that ISO 28000 shares and that structural convergence means that the distance between the

current state and a compliant supply chain security management system is smaller than a list of identified gaps might suggest. What the shared architecture does not provide is the domain specific constitution that ISO 28000 requires, the formally defined scope, the designated compliance ownership, the supply chain security specific objectives and the verification mechanisms through which contractual commitments are distinguished from substantive compliance. These are not refinements to an existing system but the foundational elements of a governance domain that does not yet exist in its own right within the organisation.

Among the most significant findings is the character of the risk that this structural condition produces. The gap between executing the Security Annex and complying with its substantive content is not discernible through operational monitoring alone and neither is the progressive accumulation of security relevant exposure by suppliers whose individual interactions remain below the thresholds that would trigger reclassification. Both conditions share the same structural characteristic in that those are detectable only through governance mechanisms specifically designed to surface them and those mechanisms do not currently exist within the supply chain security function. The practical implication is that the organisation's understanding of its actual security exposure within the supplier network may be materially less accurate than its formal governance picture suggests, not as a consequence of negligence but because the current governance architecture was not designed to render that category of risk visible.

The role of the SME group illuminates this condition from a different angle. The group performs a coordination function that is both valuable and operationally necessary. Its development in the absence of formal institutional infrastructure reflects genuine organisational capability and demonstrates that the knowledge, the professional relationships and the commitment required to govern supply chain security are present within the organisation. Its informal character means that it cannot provide the institutional continuity, the documented decision making authority and the structural guarantee of consistency that formal governance necessitates. Rather than resolving the governance gap, its existence demonstrates that the organisation already holds much of the capability required to do so.

Considered together, these findings point towards a conclusion that is demanding in its implications yet encouraging in its premise. Supply chain security governance does not need to be built from the beginning. The task ahead is rather one of making a deliberate architectural choice, to constitute supply chain security as a governed domain in its own right, with the structural conditions necessary to pursue, evaluate and improve it systematically over time. That choice requires institutional commitment and organisational investment, but it does not presuppose capabilities the organisation does not already possess. The central question is whether the governance choices made in the period ahead will reflect the strategic ambition expressed in the organisation's own

security policy and whether the structural conditions necessary to fulfil that ambition will be deliberately put in place.

7.3 Limitations of the Analysis

Several limitations shape the interpretation of the findings and acknowledging them is not a qualification of the conclusions but a condition for interpreting them with appropriate precision. The analysis is primarily grounded in the perspective of the group level functions and while representatives from other functional areas contributed to the empirical material, the findings reflect a structural and governance level picture rather than an exhaustive account of how supply chain security is understood and practised across every part of the organisation. Supply chain security maturity varies across the organisation and that variation is only partially captured in the analysis.

The scope of what could be examined was further shaped by considerations of confidentiality, which constrained access to certain categories of internal documentation and limited the level of operational detail that could be incorporated into the assessment. This represents an inherent condition of research undertaken within a security sensitive organisation and does not reduce the analytical value of the material made accessible. It does, however, mean that certain dimensions of operational practice remain beyond the scope of the analysis and outside the basis for confident assessment.

The analysis does not constitute a formal certification audit against ISO 28000. The standard is used as an analytical reference structure rather than a prescriptive compliance instrument and the gap assessment reflects the organisation's state prior to any deliberate initiative to implement it, meaning that the conclusions drawn are descriptive and analytical in character rather than certifiable in any formal sense. As a single case study, the findings are not intended to support statistical generalisation beyond the organisational context examined, but rather to provide the analytical depth and structured foundation necessary for informed decision making regarding the future development of supply chain security governance within the organisation.

7.4 Directions for Future Research

The analysis points to questions that extend beyond the scope of a single case study, several of which indicate research directions of theoretical significance and practical consequence. The principal concern relates to areas in which the existing literature provides insufficient guidance for organisations navigating the governance challenges under examination. The relationship between supply chain security maturity and ISO 28000 alignment in defence industry organisations remains insufficiently examined and comparative research across organisations operating under similarly demanding security requirements could contribute to a more generalised understanding of what conditions determine whether formal management system structures produce

substantive rather than merely procedural improvements in supply chain security governance.

The role of informal coordination structures represents a further area where research is needed. The conditions under which informal arrangements successfully substitute for formal governance, as well as the circumstances under which that substitution becomes a structural liability, remain poorly understood and this question has implications that extend well beyond the organisational context examined. The issue of accumulated risk exposure in long term supplier relationships is similarly underexamined and the governance mechanisms best suited to capturing exposure that accumulates gradually across multiple interactions and procurement cycles warrant further empirical investigation. Supply chain security governance is, at its core, a question of whether organisations are willing to invest in structures that make invisible risks visible before materialisation The governance choices organisations make determine not only their current security posture but their capacity to anticipate and respond to threats that have not yet been encountered. That question is unlikely to become less urgent.

List of References

Boréus, K. and Kohl, S. (2018). Innehållsanalys. In: Boréus, K. and Bergström, G. (eds.), Textens mening och makt: metodbok i samhällsvetenskaplig text- och diskursanalys. 4th ed. Lund: Studentlitteratur, pp. 49–90.

Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press.
Brinkmann, S. and Kvale, S. (2015). InterViews: Learning the Craft of Qualitative Research Interviewing. 3rd ed. Thousand Oaks, CA: SAGE.

Cao, M., & Zhang, Q. (2011). Supply chain collaboration: Impact on collaborative advantage and firm performance. Journal of Operations Management, 29(3), 163–180. DOI: 10.1016/j.jom.2010.12.008

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. The International Journal of Logistics Management, 15(2), 1–14. DOI: 10.1108/09574090410700275

Company X. (2020, August 21). Security policy (WHY-0018, Issue 2). Anonymised source.

Company X. (2025). Annual and sustainability report 2024. Anonymised source.

Company X. (2025a). Interim report January–March 2025. Anonymised source.

Company X. (2025b). Interim report January–June 2025. Anonymised source.

Company X. (2025c). Interim report January–September 2025. Anonymised source.

Company X. (2025d). Year-end report 2025. Anonymised source.

Company X. (2025, August 27). Supplier code of conduct. Anonymised source.

Company X. (n.d.). Annual Planning Wheel (GMS-0275). Internal document.

Company X. (n.d.). Checklist document for procurement decision points P1–P4 (5000358-093). Internal document.

Company X. (n.d.). Corporate Purchase Agreement Templates (INF-0380). Internal document.

Company X. (n.d.). Governance of the Global Management System (WHO-0070). Internal document.

Company X. (n.d.). Group Internal Audit Instructions (INF-0641). Internal document.

Company X. (n.d.). Handle Operational Findings (HOW-0031). Internal document.

Company X. (n.d.). Interested Parties Analysis (INF-0646). Internal document.

Company X. (n.d.). Manage Audits Programme (HOW-0019). Internal document.

Company X. (n.d.). Manage Communication (INF-0620). Internal document.

Company X. (n.d.). Manage Information (HOW-0089). Internal document.

Company X. (n.d.). Manage Risk and Opportunity (HOW-0025). Internal document.

Company X. (n.d.). Manage Security Incidents (HOW-0147). Internal document.

Company X. (n.d.). Management by Objectives (HOW-0134). Internal document.

Company X. (n.d.). Management Review at Group Functions (INF-1708). Internal document.

Company X. (n.d.). Management review process (HOW-0018). Internal document.

Company X. (n.d.). Marking of Information (INF-0502). Internal document.

Company X. (n.d.). Role definition document (INF-0512). Internal document.

Company X. (n.d.). Security Annual Wheel (GMS-0534). Internal document.

Company X. (n.d.). Security audits and security check ups directed at suppliers (INF-0596). Internal document.

Company X. (n.d.). Security Awareness Programme (INF-0605). Internal document.

Company X. (n.d.). Security Legal Analysis (CZ-2020-182). Internal document.

Company X. (n.d.). Security Operations Manual (INF-0506). Internal document.

Company X. (n.d.). Security Risk Assessment process (INF-0513). Internal document.

Company X. (n.d.). Standardised template for interested parties/context analyses (5000362-359). Internal document.

Company X. (n.d.). Supplier Assessment Decision Record (5000358-247). Internal document.

Company X. (n.d.). Terms of Reference for the Procurement Council (WHO-1882). Internal document.

Company X. (n.d.). Understanding the Organisation and its Context (INF-1223). Internal document.

Company X. (n.d.). Whistleblowing Policy (WHY-0035). Internal document.

Creswell, J. W., & Creswell, J. D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th ed.). SAGE.

Domingues, P., Sampaio, P., & Arezes, P. (2016). Integrated management systems assessment: A maturity model proposal. Journal of Cleaner Production, 124, 164–174. DOI: 10.1016/j.jclepro.2016.02.101

Flick, U. (2009). An Introduction to Qualitative Research. 4th ed. London: SAGE. https://vivauniversity.wordpress.com/wp-content/uploads/2014/02/flick-2009-an-introduction-to-qualitative-research-full-book.pdf

Fonseca, L. M., Domingues, J. P., Baylina, P., & Calderón, M. (2017). Management system certification benefits: Where do we stand? Journal of Industrial Engineering and Management, 10(3), 476–494. DOI: 10.3926/jiem.2350

Försvarets radioanstalt. (2024). FRA årsrapport 2024. Stockholm: Försvarets radioanstalt. https://www.fra.se/download/18.766e440918f572e7335195/1740753605133/FRA_arsrapport_2024_uppslag.pdf

Försvarsmakten. (2025). Skyddsvärden för försvaret av Sverige. Stockholm. Försvarsmakten. https://www.forsvarsmakten.se/contentassets/546bbe13064a4c739e1cbc4b5e4571f7/skyddsvarden-for-forsvaret-av-sverige.pdf

Ghadge, A., Dani, S., & Kalawsky, R. (2012). Supply chain risk management: Present and future scope. The International Journal of Logistics Management, 23(3), 313–339. DOI: 10.1108/09574091211289200

Hallikas, J., Karvonen, I., Pulkkinen, U., Virolainen, V. M., & Tuominen, M. (2004). Risk management processes in supplier networks. International Journal of Production Economics, 90(1), 47–58. DOI: 10.1016/j.ijpe.2004.02.007

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). A review of supply chain risk management: Definitions, theory, and research directions. International Journal of Production Research, 53(16), 5031–5069. DOI: 10.1080/00207543.2015.1030467

Ing, W. H., Sorooshian, S., & Hasan, M. (2019). Benefits that attract industry to implement ISO 28000 to secure supply chain. TEM Journal, 8(1), 119-124. DOI: 10.18421/TEM81-17

International Organization for Standardization. (2022). Security and resilience. Security management systems. Requirements (ISO 28000:2022). ISO.

Jüttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: Outlining an agenda for future research. International Journal of Logistics Research and Applications, 6(4), 197–210. DOI: 10.1080/1367556031000162701 6

Militära underrättelse och säkerhetstjänsten. (2025). Must årsöversikt 2024. Stockholm: Försvarsmakten. https://www.forsvarsmakten.se/contentassets/546bbe13064a4c739e1cbc4b5e4571f7/2024-must-arsoversikt.pdf

Nunhes, T. V., Bernardo, M., & Oliveira, O. J. (2019). Guiding principles of integrated management systems: Towards unifying a starting point for researchers and practitioners. Journal of Cleaner Production, 210, 977–991. DOI: 10.1016/j.jclepro.2018.11.066

Saunders, M., Lewis, P., & Thornhill, A. (2023). Research methods for business students (9th ed.). Pearson.

Spieske, A., & Birkel, H. (2021). Improving supply chain resilience through industry 4.0: A systematic literature review under the impressions of the COVID 19 pandemic. Computers & Industrial Engineering, 158, Article 107452. DOI: 10.1016/j.cie.2021.107452

Säkerhetspolisen. (2025). Översikt av den nationella säkerheten 2024-2025. Stockholm: Säkerhetspolisen. https://sakerhetspolisen.se/download/18.328c5ae9195250d81d04ad/1741953348924/L%C3%A4gesbild%202024-2025.pdf

Thomas, A.R. & Vaduva, S. (Eds.). (2015). Global supply chain security: emerging topics in research, practice and policy. Springer. DOI: 10.1007/978-1-4939-2178-2

Tummala, R., & Schoenherr, T. (2011). Assessing and managing risks using the supply chain risk management process. International Journal of Production Research, 49(16), 4743–4762. DOI: 10.1080/00207543.2010.489459

Wagner, S. M., & Bode, C. (2008). An empirical examination of supply chain performance along several dimensions of risk. Journal of Business Logistics, 29(1), 307–325. DOI: 10.1002/j.2158-1592.2008.tb00081.x

Wieland, A., & Wallenburg, C. M. (2013). The influence of relational competencies on supply chain resilience. International Journal of Physical Distribution & Logistics Management, 43(4), 300–320. DOI: 10.1108/IJPDLM-08-2012-0243

Williams, Z., Lueg, J. E., & LeMay, S. A. (2008). Supply chain security: An overview and research agenda. The International Journal of Logistics Management, 19(2), 254–281. DOI: 10.1108/09574090810895988

World Economic Fourm. (2026). Davos 2026: Special address by Mark Carney, Prime Minister of Canada. https://www.weforum.org/stories/2026/01/davos-2026-special-address-by-mark-carney-prime-minister-of-canada/

Yin, Robert K. Case Study Research and Applications: Design and Methods. 6th ed. SAGE, 2018. https://opac.atmaluhur.ac.id/uploaded_files/temporary/DigitalCollection/YTE3NDlmYTY0ZjE2MDA5ODE4NGI1Y2FhMjdkMjRmYWNkMDA2MTVhOQ==.pdf

Żurawski, S., Ciekanowski, Z., Pauliuchuk, Y., & Ratter, E. (2025). The impact of supply chain security management on the functioning of modern organizations. European Research Studies Journal, 28(1), 44–56. DOI: 10.35808/ersj/3889

Appendix 1. Interview Guides

In addition to the formal interviews, an ongoing dialogue was maintained with Respondent 1 throughout the research process.

Interview Guide for Respondent 3

1. Could you describe your interpretation of Annex SL and how ISO management system standards could be understood within the organisational context of the company?
2. Could you describe the process of implementing ISO 27001 within the company's security management system?
3. Could you explain how the management system operates within the company and how it is applied at business unit level?
4. Could you provide a more detailed description of the management review process?
5. How do you assess the possibility of integrating ISO 28000 into an existing management system, such as ISO 27001, which the organisation is currently in the process of adopting?

Interview Guide for Respondent 7, 8, 9 & 10

1. Could you describe how the supply chain security system is applied in practice within your functional area?
2. To what extent is supply chain security integrated into procurement processes and project management activities?
3. Could you describe how risk assessments are conducted in practice, from initial assessment to follow up?
4. How is it ensured that established procedures are followed consistently over time?
5. To what extent are supply chain security practices harmonised across the different functional areas and where do differences remain? Could you also describe how collaboration takes place, particularly within the SME group?
6. When acting as a security expert in support of procurement processes, could you describe your role and the process involved? Are there significant differences between buyers in how security requirements are handled, or does the current procurement model support consistent application?

Interview Guide for Respondent 4, 5, 6, 12, 13 & 14

1. Could you describe the function and category area in which you work?
2. How are security requirements addressed during supplier approval, procurement activities and contract establishment?

3. How familiar is your department with supply chain security? Is it an area that you actively work with, or are you primarily required to comply with established requirements?
4. Are you aware of any deviations from standard procedures in practice, despite the formal guidelines set out in the GMS and internal documents? For example, do purchasers apply different working methods while still operating within the established framework?
5. How do you perceive the current risk management process? How is compliance managed and do you consider the process effective, or are there aspects that require further development?
6. How do you perceive the Security Annex? Is it clear and practical to apply and what challenges do you commonly encounter in relation to it?
7. In which areas would additional support have been beneficial regarding supply chain security within the procurement process?

Interview Guide for Respondent 2, 11 & 15

1. How do you perceive the current risk management process? How is compliance managed and do you consider the process effective or are there aspects that require further development?
2. Could you describe the process for risk and sanctions screening, including the main factors considered during the assessment?
3. What procedures should be followed if discrepancies or concerns are identified during the background check?
4. What types of measures could the company take if the outcome of the assessment is not fully satisfactory?
5. Are there any additional aspects that the supply chain security function may wish to include in the screening process?
6. Could you describe how ongoing supplier communication is structured and how security incidents are managed and escalated?

DEPARTMENT OF TECHNOLOGY MANAGEMENT AND ECONOMICS
DIVISION OF SUPPLY AND OPERATIONS MANAGEMENT
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2026
www.chalmers.se

CHALMERS
UNIVERSITY OF TECHNOLOGY