CHALMERS
UNIVERSITY OF TECHNOLOGY

A study of the Gothenburg Tramways system with a focus on Crisis Preparedness and Risk Management

Ensuring Compliance with NIS2 and CER Directives through Procurement and Supplier Relationships

Master's thesis in Design and Construction Project Management

ALBIONA BERISHA
SHIHAN ELMI

DEPARTMENT OF SOME SUBJECT OR TECHNOLOGY
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2025
www.chalmers.se

Master's thesis 2025

A study of the Gothenburg Tramways system with a focus on Crisis, Preparedness, and Risk Management

Ensuring Compliance with NIS2 and CER Directives through Procurement and Supplier Relationships

ALBIONA BERISHA
SHIHAN ELMI

CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Architecture and Civil Engineering
Chalmers University of Technology
Gothenburg, Sweden 2025

A study of the Gothenburg Tramways system with a focus on Crisis, Preparedness, and Risk Management

Supervisor: Daniella Troje, Department of Architecture and Civil Engineering
Examiner: Daniella Troje, Department of Architecture and Civil Engineering

Master's Thesis 2025
Department of Architecture and Civil Engineering
Chalmers University of Technology
SE-412 96 Gothenburg
Telephone +46 31 772 1000

A study of the Gothenburg Tramways system with a focus on Crisis, Preparedness, and Risk Management
Ensuring Compliance with NIS2 and CER Directives through Procurement and Supplier Relationships
ALBIONA BERISHA
SHIHAN ELMI
Department of Architecture and Civil Engineering
Chalmers University of Technology

Abstract

This thesis examines how the City of Gothenburg's tramway procurement and supplier relationships can be organized to ensure compliance with the EU's NIS2 and CER directives. Using a qualitative case study approach with semi-structured interviews of key municipal and supplier stakeholders, the study identifies gaps in awareness, governance, supplier readiness, contract design, and leadership engagement. Findings indicate that effective implementation requires formal governance structures, role-specific training, procurement criteria aligned with criticality levels, flexible contractual clauses, clear information classification, and sustained leadership. The study proposes actionable recommendations and outlines opportunities for future research, including longitudinal effects, SME-adaptability, and frameworks for sensitive data protection.

Keywords: NIS2-directive, CER-directive, Procurement, Supply management, Crisis prepardness and Tramway system.

Acknowledgements

Firstly, we would like to express our heartfelt gratitude to our supervisor Daniella Troje for her support and guidance during this time. Her insightful feedback and support helped us through our research and brought this work to completion. Additionally, we are thankful to the faculty and professors at the department of Architecture and Civil Engineering at Chalmers for creating an environment that encouraged both academic growth and critical thinking throughout our studies. We also thank our supervisor at the City of Gothenburg's Urban Environment Department for their invaluable assistance with interviews, and ongoing support throughout this project. As this marks the end of our journey as students at Chalmers, we sincerely thank our families and friends for their unwavering support throughout our years of study. Your encouragement, patience, and belief in us have meant more than words can express.

Contents

1
Introduction

This chapter outlines a brief background to the NIS2 and CER directives as well as focuses on the purpose, limitations, research questions and methodology of the report.

1.1 Background

The global security situation in 2025 is characterized by increasing uncertainty, with a large number of ongoing conflicts and growing tensions (Elsner et al., 2025). Geopolitical developments like the situation in Ukraine and the rising tensions in the Middle East have had a direct impact on global stability. According to the Swedish Security Service (SÄPO), the current terrorist threat level is assessed at four out of five, indicating a high risk of security incidents. This shift is creating new and complex challenges for global security and adding to these concerns is the growing reliance on technology in modern conflicts. The rise in cyberattacks, sabotage, and political influence campaigns has exposed vulnerabilities within critical infrastructure and key societal functions.

Ensuring security is crucial not only to protect lives and health but also to maintain societal function and uphold core values (MSB, 2012). One of the key components of a functioning society is transportation infrastructure, enabling the flow of goods and people (Dong, Shan & Hwang, 2022). With increasing vulnerability, transport infrastructure is facing more risks from natural disasters and human-made threats. The growing interconnectivity of transport systems also raises the chances of chain reactions when disruptions occur (Serdar, Koç & Al-Ghamdi, 2022). Events like cyberattacks or power failures can escalate quickly and affect several systems at once.

Addressing these emerging challenges has become a priority for the European Union. In June 2024, the EU established its political priorities for the upcoming years, emphasizing the importance of security and defense, particularly in relation to both physical and digital threats (European Union, n.d.). As part of these efforts, the EU has introduced two new directives: NIS2 (Network and Information Systems Directive 2) and CER (Directive on the Resilience of Critical Entities) (Regeringskansliet, 2024a). Member states were required to implement the necessary national legislation to comply with these directives by 17 October 2024. The NIS2 directive updates the original NIS directive from 2016, with a focus on improving cybersecurity throughout the EU. Meanwhile, the CER directive replaces the previous European Critical

Infrastructure (ECI) directive and aims to enhance the resilience of essential services and critical infrastructure against various threats.

The updated directives introduce several important changes. They extend their scope to include additional sectors, such as transportation, and impose stricter requirements for the protection of network and information systems (Sveriges Kommuner och Regioner, 2024). Furthermore, the regulations apply to public administration and essential services, including municipalities, regions, and other key sectors. Organizations operating in these areas are required to register with the appropriate authorities and report any incidents, with supervisory responsibilities varying depending on the specific sector.

For municipalities like Gothenburg, this represents a major change. The city's tramway system, a vital part of its infrastructure, is now covered by the NIS2 and CER directives, which previously did not apply to tramways. Owned by the City of Gothenburg and managed by the Urban Development Administration, this department is responsible for procurement, planning, construction, and operations. Since many different actors are involved in the tramway's supply chain, it is essential that both the municipality and its suppliers comply with the security requirements set out in the directives. To comply with the new requirements, the city must restructure its processes and working methods.

1.2 Purpose and Research question

The purpose of this study is to critically assess the tramway system's alignment with the new security requirements outlined in the NIS2 and CER directives. The research will explore the role of procurement and supplier management in facilitating the implementation of these regulations, using a systems approach to analyze how organizational structures and processes can be optimized for enhanced security and resilience.

The main research question for this project is:

How can procurement and supplier relationships be organized to ensure the tramway system meets NIS2 and CER?

The findings will be adapted and applied to the context of urban infrastructure development to identify best practices and inform recommendations for improvement.

1.3 Limitations

This report will not address technical solutions in detail for every aspect of the NIS2 and CER directives. The primary focus will be on procurement and supplier relationships and how these can be organized to support compliance with the directives.

External factors affecting the system, but not directly related to procurement and supplier relationships, will not be covered.

2

Literature review

This chapter presents a literature review of the central topics explored in the study. It begins with an overview of the new EU directives NIS2 and CER, highlighting their scope, similarities, differences, and implementation challenges. The review then examines the vulnerability of transport infrastructure and introduces the concept of resilience. Finally, it explores key themes related to cybersecurity in supply chains and the complexities of public procurement under confidentiality requirements.

2.1 NIS2- and CER-directive

The European Union implemented several new legislative measures that are designed to enhance the resilience and protection of network and information systems as well as critical entities across the union (Mikac, 2023). NIS2 (Network and Information Systems Directive 2) is a legislation and plays a central role in improving cyber security across the EU. The CER-directive (Directive on the resilience of critical entities) is a legislation that seeks to enhance physical security of critical entities. These two directives are applied in parallel and have mutual references which means that any weaknesses in one could substantially affect the implementation of the other.

2.1.1 NIS2-directive

The NIS2-direcive strengthens the cybersecurity requirements and introduces the concepts of “essential” and “important” entities, replacing “operators of essential services” and “digital service providers” (National Cyber Security Centre, n.d). The classification of “essential” and important are based on factors such as size, sector, and criticality. Examples of essential entities are energy and transport sectors. These are entities that are critical for a functioning society. On the other hand, “Important” entities are organizations that are less critical than “essential” and could be certain types of digital infrastructure . Additionally, other sectors of wide criticality are health and water systems. There have also been a few ad ins to this category like Space and Public admin. In both important and essential entities senior management is responsible for cybersecurity risk management (National Cyber Security Centre, n.d). If the management does not comply with NIS2 requirements there will be repercussions including liability, temporary bans and administrative

fines. Management bodies should:

- Approve adequacy of the cybersecurity risk management measures taken by the entity.
- Supervise the implementation of the risk management measures
- Follow training in order to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the entity
- Offer similar training to their employees on a regular basis
- Be accountable for the non-compliance

The Swedish Civil Contingencies Agency (MSB) plays a vital role in enhancing the cybersecurity posture of Sweden's public sector (Rehnstam et al., 2025). With the continuous increase of cyberthreats, strong information security measures and competences are becoming increasingly essential. In addition, MSB has developed initiatives such as "Cybersäkerhetskoll and Kompetensförsörjning" to evaluate and enhance the cybersecurity preparedness and capabilities of Swedish organizations.

2.1.2 CER-directive

The CER Directive is designed to improve the resilience of essential services and imposes obligations to implement measures that guarantee their strength and stability (MSB, 2023). Critical sectors refer to functions, services, and infrastructures that are essential for maintaining societal functions necessary for public safety and stability, such as energy, transport, financial services, and healthcare. These sectors, which are operated by both public and private entities, are fundamental for society to function safely and stably. The directive covers critical sectors such as energy, transport, finance, healthcare, drinking water supply, sewage, digital infrastructure, public administration, and space technology. According to the directive, member states are required to ensure that critical sectors have the capacity to manage and recover from disruptions or interruptions, whether caused by natural disasters, pandemics, terrorism, or other serious events.

To achieve this, the directive sets several specific requirements and measures:

- requires each member state to develop a national strategy to strengthen the resilience of critical sectors, with clear goals and priorities.
- A risk assessment must be conducted to identify threats within various sectors and subsectors.
- Entities responsible for critical operations must be identified, and a consequence analysis in case of failure must be conducted.

- Member states must designate one or more competent authorities responsible for implementing and monitoring compliance with the directive.
- Entities designated as critical must take technical, organizational, and security measures proportional to the identified risks.
- Incidents that may cause significant disruption must be reported to the competent authority.
- Entities providing services in at least six member states may be granted a special status as critical entities of European importance, which entitles them to specific support.
- The European Commission will provide support to both member states and critical entities.

In Sweden, the Swedish Civil Contingencies Agency (MSB) plays a key role in implementing the CER Directive (Regeringskansliet, 2024b). As the national contact point, MSB coordinates supervisory authorities, handles incident reports from critical operators, and carries out national risk assessments. It is also responsible for forwarding notifications about operators that are considered particularly significant at the European level.

The CER Directive replaces Directive 2008/114/EC, which primarily focused on identifying and designating European Critical Infrastructure (ECI) within the energy and transport sectors (Regeringskansliet, 2024b). According to Regeringskansliet (2024) the EU has been working for years to improve the protection of critical infrastructure, but previous regulations have been too narrow, addressing only specific sectors and certain aspects of resilience. This limited approach has proven insufficient in preventing disruptions. As a result, the focus has now shifted from simply protecting individual infrastructure assets to ensuring that organizations providing essential services are resilient enough to withstand and recover from potential threats.

2.1.3 Similarities Between the Directives

The NIS2- and CER-directives share several common features in their structure (Regeringskansliet, 2024b). Both directives cover the same sectors and define public administration entities at the national level in an identical manner. Operators classified as critical under CER are also considered essential under NIS2. Oversight of both directives should be handled by the same authority, ensuring consistent supervision. Incident reporting to MSB is coordinated for operators that fall under both regulations. Both NIS2 and CER require the maintenance of confidentiality and the reporting of incidents. Entities identified as critical under CER are also regarded as essential under NIS2. Furthermore, the relevant authorities for each directive must cooperate and exchange information on threats, incidents, and the measures taken in response.

2.1.4 Differences Between the Directives

The NIS2 and CER directives protect different aspects of critical operations and have distinct focus areas (Regeringskansliet, 2024b). The NIS2 directive is aimed at safeguarding network and information systems, while the CER directive focuses on protecting critical infrastructure. A business operator that has implemented risk management measures to protect an information system according to NIS2 may still be required to take broader measures under the CER directive. These measures may include both physical security and continuity for the critical service. The sectors covered by the CER directive are also found in NIS2, but NIS2 includes additional areas not covered by CER, such as postal and courier services and waste management. The differences between the directives also impact how the impact assessment should be conducted. To be covered by NIS2, it is sufficient for an operator to belong to a designated sector according to the annexes of the directive. However, to be covered by CER, the operator must both belong to a designated sector and be identified as critical, making the requirements more comprehensive.

2.1.5 Challenges in Implementing the Directives

The implementation of the NIS2 and CER directives presents a range of challenges that can make their practical application more difficult (Mikac, 2023). The main issue lies in the complexity of the directives and the short 21-month transposition period, which ended on 17 October 2024, potentially leading to non-compliance and operational difficulties. Furthermore, there is a lack of clear definitions and established processes for crisis management in both directives, making it harder to apply them in a consistent and effective manner. Another problem is that the NIS2 directive does not adequately consider emerging threats, such as artificial intelligence and quantum computing. This means that potential future security risks are not properly addressed, which could reduce the long-term relevance and effectiveness of the directive. In addition, the directives cover a wide range of sectors and activities, with many actors classified as critical. This can lead to varying interpretations of the rules and create a significant administrative burden for both public and private sectors. Countries with weak cybersecurity systems may also struggle to meet the requirements set by NIS2, risking an uneven level of protection across the EU. Moreover, differences in the interpretation and understanding of the directives among actors both within and outside the EU can lead to fragmented and inconsistent implementation. Another challenge is the lack of clear guidelines for information exchange in crisis management. The focus is primarily on operators reporting to authorities and the commission, while there are no structured processes for feedback in the opposite direction.

2.2 Threats and Resilience in Transportation Infrastructure

Transportation infrastructure is essential for modern society as it enables the movement of people and goods (Dong, Shan & Hwang, 2022). However, this infrastruc-

ture is vulnerable to both natural disasters and human-made threats. Events like the 2011 tsunami in Japan demonstrated how quickly roads, bridges, and railway systems can be damaged, causing major disruptions for communities. This has led to increased focus on strengthening the resilience of transportation systems, meaning their ability to resist, recover from, and adapt to different types of disturbances.

In addition to the challenges posed by natural events, deliberate attacks, both physical and cyber, pose a significant threat to transportation infrastructure (Serdar, Koç & Al-Ghamdi, 2022). These attacks are often driven by political or economic motives and typically target critical or symbolic infrastructure, particularly in conflict areas.

One study highlights that in the event of a terrorist attack targeting a large railway network, authorities are likely to shut down parts of the system, disrupting its operations (Serdar, Koç & Al-Ghamdi, 2022). The effects of such attacks can be significant, economically, socially, and politically, with long-lasting consequences. As modern transportation networks are highly interconnected, the risk of cascading failures increases, where a single disruption, such as a cyberattack or power outage, can spread and affect multiple systems at once. This makes it even more important to prioritize resilience, which requires continuous monitoring, risk assessment, and careful analysis of potential threats.

Digitalization is a key trend within the transportation sector, involving the integration of information and communication technology (ICT) into both administrative functions and technical infrastructure (Dokuchaev & Maklachkova, 2023). This technology improves logistics, resource utilization, and decision-making, leading to lower costs and a more efficient supply chain. As transportation companies handle large amounts of personal data, information security becomes increasingly important.

However, the rise of digitalization is also changing the threat landscape for transportation security (Dokuchaev & Maklachkova, 2023). In addition to protecting physical infrastructure, companies now must also protect their digital systems. The transportation sector, as part of critical infrastructure, is an attractive target for cyberattacks. Railway systems, in particular, are vulnerable because their control systems for signaling, traffic management, and passenger information rely on both IT and operational technology (OT). Manipulating these systems could lead to severe consequences, such as traffic disruptions or accidents. Cyberattacks can result in financial losses, security risks, and damage to a company's reputation. Therefore, it is essential for organizations to understand the growing cyber threats and develop strategies, policies, and technical solutions to protect their digital systems.

2.3 Cybersecurity in the Supply Chain

The updated NIS2 directive imposes increased demands on organizations within the EU to strengthen their cybersecurity efforts, not only internally but also in relation to external dependencies such as suppliers and service providers (ENISA, 2022). As

a result, cybersecurity efforts can no longer be confined to an organization's internal IT environment but must instead encompass the entire digital ecosystem. According to ENISA, the European cybersecurity agency, this work should be grounded in a risk-based approach that includes the entire supplier landscape.

To understand what this means in practice, it is important to define what a supply chain is. Supply chain management can be defined as a "linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling and delivery of products and services to the acquirer" (University of Oslo, 2023). A supply chain, therefore, consists of a network of actors who collaborate to develop and deliver products and services to end users.

Within this network, the so-called focal company plays a central role (Ship, 2024). This is the company responsible for designing the product, maintaining direct contact with the customer, and coordinating the various parts of the chain. First-tier suppliers have a direct relationship with the focal company and often provide key components such as network chips, cameras, batteries, or core software. In some cases, these first-tier-suppliers are also responsible for assembling the complete product for the focal company. Focal companies typically manage or oversee the supply chain, maintain direct contact with the customer, and design the products or services offered. Additionally, they hold the main responsibility for the operation of the supply chain, which means thats that they often oversee and enforce cybersecurity measures within the supply chain

However, even first-tier suppliers rely on multiple layers of sub-suppliers, such as second-tier suppliers, resulting in a complex and often non-transparent supply chain structure that is difficult to monitor and control (see figure 2.1) (Ship, 2024). The further a supplier is from the focal company, the more difficult it becomes to assess their cybersecurity posture. Even companies with strong internal security systems may be vulnerable if a supplier with network access fails to meet cybersecurity standards.

The NIS2 directive emphasizes this need by outlining specific security measures, covering both technical and organizational requirements, for essential and important entities (University of Oslo, 2023). It also highlights the importance of considering the physical environment, such as protection from fire, flooding, and theft, as part of the broader protection of networks and information systems.

To meet these requirements, organizations must adopt a sustainable approach to managing supplier risks (ENISA, 2022). This includes continuous monitoring of changes in suppliers' operations, such as new ownership structures, shifts in technology use, or security incidents. Such changes can rapidly alter the risk landscape and may necessitate actions like renegotiation or termination of cooperation. Clearly defined security requirements should be set already in the procurement phase. These may include demands for certifications, established procedures for vulnerability management, incident reporting, and protection of sensitive data. By setting these ex-

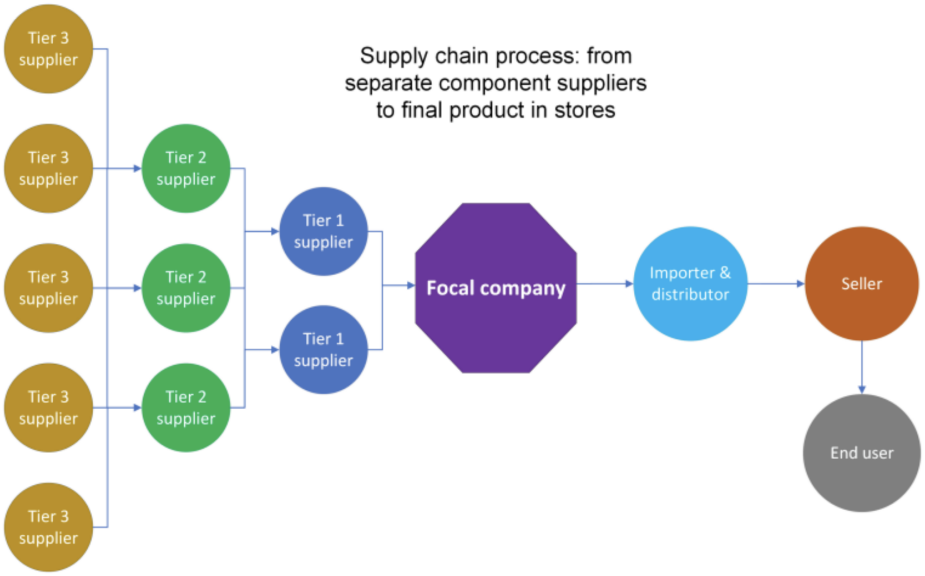

Figure 2.1: Multi-Tier Supply Chain (Ship,2024)

pectations early on, a secure and predictable supplier relationship can be established and maintained throughout the entire supply chain.

It is becoming increasingly important to include clear cybersecurity requirements in the supplier selection process (Jan et al., 2023). The ability to demonstrate compliance with cybersecurity standards has become a critical factor in supplier evaluations. However, this also presents challenges for small and medium-sized enterprises (SMEs), which face significant difficulties in the supply chain due to complex questionnaires, limited resources, and high costs. Larger companies often require SMEs to complete detailed, time-consuming questionnaires that vary by client, along with providing extensive documentation, such as cybersecurity policies. Without the necessary expertise, SMEs often need to hire costly consultants to meet these demands.

Additionally, the financial burden of upgrading cybersecurity can be overwhelming (Jan et al., 2023). While basic protections are affordable, more advanced solutions like network segmentation and cloud-based services are costly, yet necessary to ensure security and maintain customer trust. This financial strain, coupled with the complexity of compliance, makes it difficult for SMEs to meet larger organizations' expectations, despite the critical need for securing the entire supply chain.

2.3.1 Strengthening Cybersecurity Resilience in Supply Chains

As digitalization continues to expand, cybersecurity has become an increasingly central issue, particularly when it comes to protecting critical infrastructure, with special focus on vulnerabilities within software supply chains (Raponi et al., 2021). Digitalization of vital systems has introduced new systemic risks, particularly through vulnerabilities found in software supply chains. Today's critical infrastructures are heavily reliant on advanced information technology, where each component, from

hardware to cloud services, can become a potential target for cyberattacks. This has led to a situation where the attack surface for cyber threats is constantly expanding, while security solutions have struggled to keep pace with this development.

Raponi et al. (2021) emphasize that software updates and digital communications in these environments are often implemented without sufficient verification, increasing the risk of malicious code spreading through the supply chain. A serious incident that illustrates this is the SolarWinds attack, where hackers from the Russian APT29 group (Cozy Bear) infiltrated the global IT supplier SolarWinds, leading to extensive breaches at various U.S. government agencies and major tech companies. This attack underscores the need not only to protect internal systems but also to secure the entire supply chain, including external actors that provide software and updates.

In line with these technical and systemic challenges, Nweke and Wolthusen (2020) in their article discuss how legal and organizational barriers to information sharing hinder private companies from cooperating effectively on cybersecurity issues (Nweke & Wolthusen 2020). They point out that cybersecurity collaboration is of utmost importance because cyberattacks often impact entire global supply chains, and quick information sharing is crucial to prevent the spread of threats. However, despite this, companies often face significant obstacles. Businesses are reluctant to share security-related information due to risks associated with privacy laws, data protection regulations like GDPR (General Data Protection Regulation), and competition laws, which can undermine effective cooperation and defense against cyber threats. To address these barriers, Nweke and Wolthusen (2020) suggest that clearer legal guidelines and protections are needed for companies that want to collaborate on cybersecurity. They also emphasize the need for more comprehensive cooperation between private and public actors to create legal frameworks that encourage information exchange without compromising businesses' commercial standing.

A comparison between the United States and Norway illustrates how different countries handle these challenges (Nweke & Wolthusen 2020). The U.S. has, through legislation such as the Cybersecurity Information Sharing Act (CISA) of 2015, introduced legal protection for companies voluntarily sharing cyber threat information, which has created an environment where collaboration is encouraged rather than discouraged. In contrast, Norway has a more cautious and decentralized model, where cooperation often takes place through voluntary agreements supported by the Norwegian National Security Authority (NSM). This uncertainty can lead to passivity and weaken cybersecurity, especially in cross-border situations.

Furthermore, Sadeghi, Azadegan, and Ojha (2023) argue that technical solutions alone are not enough to build resilience against cyber threats. Their research shows that to enhance resilience in supply chain networks, companies must also develop organizational capabilities. Two key concepts that are crucial for this are absorptive capacity and visibility, which refer to a company's ability to absorb and apply new information and the transparency and visibility of information within the supply chain (Sadeghi et al., 2023). Companies with higher absorptive capacity tend to have greater visibility within their supply networks, making it easier to identify and

manage risks at an early stage. This is particularly important because it can be difficult to protect the entire supply chain if not all actors share information about their own vulnerabilities and security measures.

Another important aspect highlighted in the study is how the power balance between buyers and suppliers affects the flow of information (Sadeghi et al., 2023). When the buyer holds a stronger position in the relationship, they can impose higher requirements for information sharing and security, which enhances transparency across the chain. On the other hand, if the supplier holds more power, they may be less willing to share security-related information, which can complicate collaboration and weaken security efforts across the entire chain. The authors stress that cybersecurity is not only an internal matter. Even if a company has robust internal security measures, the entire chain can still be vulnerable if suppliers do not share relevant information about their own security practices or vulnerabilities.

Finally, the experimental part of Sadeghi et al.'s study (2023) reveals that factors such as the timeliness and accuracy of information are crucial for how companies can respond to cyber incidents. Delayed or inaccurate information can lead to uncertainty, making decision-making more difficult and ultimately weakening the resilience of the entire chain. This insight is central to understanding how important it is to have both quick and correct information to recover from cyberattacks and to prevent severe consequences for both individual companies and the entire supply network.

2.4 Security, Secrecy, and Supply Chain Resilience

Defense procurement is a complex field where legal and political considerations are closely connected (Hellberg & Lundmark, 2025). Within the European Union, legal systems have been designed to promote transparency and fair competition between companies. However, in practice, this has often led to price becoming the main selection criterion. Over time, this has shaped a procurement culture based on short-term contracts and transactional relationships.

The EU treaties include rules that allow member states to bypass standard procurement procedures in matters of national security (Hellberg & Lundmark, 2025). This flexibility enables countries to protect strategic production, which has become increasingly important as new threats arise and the need for self-sufficiency grows. The rising demand for defense equipment has exposed weaknesses in the cost-driven model and put pressure on global supply chains. In response, there has been a shift in focus toward resilience, delivery security, and long-term strategic partnerships. Both at the EU level and within individual member states, new initiatives have started to support the defense industry with financial aid and more flexible procurement practices. These efforts challenge the previous focus on open competition and instead aim to allow more strategic cooperation. Approaches like direct contracting, targeted funding, and partnership models are now becoming more widely accepted in the defense sector.

Defense procurement is also shaped by specific demands, especially around confidentiality, security, and the state's control over sensitive matters (Hellberg, 2023). Classified information is treated as a top priority throughout the procurement process, and it is essential that security is maintained all along the supply chain. Any acquired equipment must meet the necessary standards for protecting sensitive information and maintaining safety.

Carrying out this kind of procurement involves several challenges (Hellberg, 2023). One of the most difficult parts is finding the right balance between the need for transparency, which supports competition, and the need to protect confidential information. Ensuring that foreign suppliers meet Swedish security requirements can be both legally and practically challenging. Other difficulties include complex regulations, limited resources, lack of relevant expertise, and decision-making processes that are slow and require a lot of effort. Protecting classified information is also complicated, as it requires security checks on all involved, including organizations and individuals. To reduce the risk of leaks, selective procurement is often used. In this process, only a few pre-approved suppliers are allowed to participate. This ensures that all parties meet the necessary security standards. High demands are also placed on information security throughout the supplier chain. Protective measures like encryption, separate networks, and controlled access to digital platforms are used to safeguard defense-related data.

The swedish security protection legislation sets clear requirements for how sensitive operations must be managed when external parties are involved (Säkerhetspolisen, 2023). If another organization is to gain insight into or access security-critical activities, a thorough preliminary assessment must be carried out. This process is used to identify which assets need protection, what risks are involved, and whether the planned cooperation can be justified from a national security perspective. When the other party may come into contact with information or activities that are considered important to national security, a security protection agreement is required. This agreement must clarify how the protection of information, personnel and physical environments will be maintained. Even if parts of the work are assigned to an external party, the main organization retains full legal responsibility.

The form and scope of the agreement depend on where and how the external party gains access (Säkerhetspolisen, 2023). There are three levels reflecting the degree of exposure. The highest level applies when access occurs outside the controlled areas of the main organization, while lower levels apply when access takes place within protected spaces or in an indirect way. Individuals working for the external party, particularly those handling or being present near sensitive information, must go through careful background checks. This often includes a formal security screening and record check. These requirements also apply to subcontractors, who must have their own agreements in place if they are given access to the sensitive material or operations.

The responsible organization must ensure that the external party complies with the agreement (Säkerhetspolisen, 2023). This is done through regular evaluations and

follow-ups. If shortcomings are identified, they must be documented and addressed. If the issues are not resolved, the supervisory authority has the right to halt the cooperation. Once the cooperation comes to an end, all sensitive information must be handled securely. This includes returning or destroying classified materials and removing all access rights. The main organization is also responsible for making sure the other party is aware of any ongoing confidentiality obligations that remain after the collaboration ends. Finally, it is crucial to evaluate whether the external party is a suitable partner in the first place. Previous violations of security rules or uncertainties regarding the structure of the organization may be strong reasons to avoid cooperation, as such weaknesses could pose serious risks to Sweden's national security.

3

Methods

In the following section, the methodological approach of the report is presented. The approach used to address the research question is described, covering aspects such as data collection, analysis, and the overall research strategy. This section also includes an introduction to the Municipality of Gothenburg, highlighting collaboration and responsibility in Gothenburg's tram system development and operation, as well as an overview of public procurement in Sweden and the City of Gothenburg.

3.1 Research approach

This study uses a qualitative research approach in order to assess the tramway system's alignment with the new security requirements outlined in the NIS2 and CER directives. Qualitative research methods are important for gaining deep understanding and exploring complex topics (Lim, 2024). The report includes interviews as the main data collection.

Moreover, in qualitative research, two primary approaches are used: inductive and deductive (Ayton, 2023). This research is conducted in collaboration with the Urban Environmental Department of Gothenburg City, which was selected as the case study due to its responsibility for overseeing the operation and procurement of the tramway system in Gothenburg. Additionally, this study adopts an inductive approach with a qualitative research method and uses interviews as the primary data collection. This approach allows the research to focus on the participants. Inductive approach is guided by participants and their data, taking a broad perspective that incorporates social and historical contexts. It examines various layers influencing individuals, such as temporal, spatial, institutional, and structural factors, while emphasizing meanings, ideas, and lived experiences (Ayton, 2023). The focus is on participants' subjective perspectives, and when analyzing interview data, researchers identify emerging themes without imposing prior assumptions. The reason for the selection of this approach is to get a better understanding of the perspectives of stakeholders and suppliers involved in the procurement process of tramway systems. This then shapes the patterns that are grounded in the real world experience. Moreover, an inductive approach avoids imposing predefined frameworks on the data and allows interviewees to define what challenges they encounter with the directives in regards to the procurement process (Ayton, 2023).

Data for this study was primarily collected through semi-structured interviews (see Appendix 1 for the interview questions). This method provides a consistent framework across interviews while allowing for deeper exploration when new or relevant topics arise during the conversation (DeJonckheere & Vaughn, 2019). A total of 11 interviews were conducted with key stakeholders. These included representatives from Gothenburg's tramways (Göteborgs spårvägar), the municipality, and Infracontrol, with expertise in areas such as cybersecurity, crisis preparedness and tramway systems (see Table 3.1). Furthermore, the interviews lasted approximately 30-40 minutes each and some were digital meetings and others were in person. Participants' were informed about the purpose of the study and why they were asked to partake in it. Additionally, consent to record for later transcriptions were requested and granted for all interviews. The material was then analysed and reviewed to identify recurring themes related to compliance to NIS2 and CER from a procurement perspective.

Interview participants	**Role**	**Organisation**
A1	Planning manager signal	Urban Environment Department
A2	IT procurement officer	Urban Environment Department
A3	Information security coordinator	Urban Environment Department
B1	Crisis and preparedness manager	Göteborgs Spårvägar
A4	Security coordinator	Urban Environment Department
B2	Information security coordinator	Göteborgs Spårvägar
B3	Security manager	Göteborgs spårvägar
A5	Infrastructure manager industrial tracks	Urban Environment Department
A6	Coordinator for track safety	Urban Environment Department
A7	IT object manager	Urban Environment Department
C1	System developer	Infracontrol

Table 3.1: Overview of interviewees, their roles, and organisations

In addition to conducting interviews, a literature review was performed by searching academic databases such as Google Scholar, Scopus, and ResearchGate. Searches were conducted using both English and Swedish keywords to identify relevant studies. Key terms included NIS2, CER, cybersecurity, supply chain, and procurement. During this thesis, a chatbot was used to assist with different parts of the writing process. It helped by editing text to make it clearer, and suggesting better ways to write sentences. For example, prompts such as "Rewrite this paragraph to make it flow better and avoid repeating words" were used to improve the text.

3.2 Municipality of Gothenburg

The City of Gothenburg operates through a well-organized network of administrations and municipal companies, all working together to guide the city's growth and provide essential public services (Göteborgs Stad, n.d.-a). Overseeing this system is the City Executive Office, which ensures that decisions made by the City Executive Board are carried out effectively and in line with the city's goals. At the top of the decision-making chain is the City Council, responsible for setting the city's most important guidelines and long-term objectives. The City Executive Board then takes on the role of making sure those decisions are implemented properly, regularly monitoring and evaluating progress along the way. The city's administrations are divided into different areas, each handling critical functions like education, transportation, and urban planning. Besides these public services, several municipal companies work in areas such as housing and culture. To keep everything running smoothly and ensure proper procedures are followed, the City Audit Office frequently reviews the work of the City Executive Board, various committees, and municipal companies.

The City Environment Administration is responsible for developing and managing Gothenburg's public spaces while working to improve the city's accessibility (Göteborgs Stad, n.d.-b). Their goal is to create safe and accessible environments where residents can thrive. They oversee areas such as the city's parks, squares, waterways, bridges, and quays, ensuring that the infrastructure for roads, pedestrian and bicycle paths, and tram tracks operates smoothly and continues to evolve.

3.2.1 Collaboration and responsibility in Gothenburg's tram system development and operation

The development and operation of the tram system in Gothenburg relies on a complex collaboration among several key stakeholders, all working towards the goal of creating an efficient and safe tram service (Göteborgs Stad, n.d.-c). Responsibilities and tasks are defined by permits from the Swedish Transport Agency and various agreements and direct allocations between the involved parties. The primary actors in this collaboration include Gothenburg City, the Västra Götaland Region, and Gothenburg Tramways. Within Gothenburg City, the Urban Environment Department holds the overall responsibility for tram track ownership. In addition to these central actors, smaller parties also play a crucial role in maintaining an effective tram network through various partnerships and specific tasks.

Below are the main areas of responsibility and the actors involved:

- **Trams:** Västtrafik is responsible for owning the majority of the trams and ensuring their long-term maintenance and care.
- **Tracks:** Urban Environment Department owns and manages the infrastructure for the tracks, which are part of the city's tram network.
- **Tram stops:** The tram stops are owned and managed by the Urban Environ-

ment Department, which ensures they are properly maintained and accessible for passengers.

- **Track layout:** The planning and decision-making regarding new or modified tram lines is a collaborative process involving several parties, including the Västra Götaland Region, Urban Environment Department, Västtrafik, and Göteborgs Spårvägar. Long-term planning is a key component of this process.
- **Contact wires:** The Urban Environment Department is responsible for both the ownership and management of the contact wires. Meanwhile, Göteborgs Spårvägar handles the operation and maintenance of these wires.
- **Power supply:** The Urban Environment Department owns and manages the rectifier stations, while Vattenfall is responsible for their operation and service. Göteborg Energi supplies the electricity required for the tram system.
- **Depots:** The tram depots are owned by the Västra Götaland Region and managed by a dedicated unit responsible for property services and support.
- **Track works:** The Urban Environment Department is in charge of organizing and planning track repairs and reconstructions. These works are carried out either by Göteborgs Spårvägar or external contractors. To carry out track work, suppliers must undergo specialized safety training, which is administered by the City Planning Department.

3.2.2 Public Procurement in Sweden and the City of Gothenburg

Swedish public procurement is regulated by procurement legislation, which is based on common EU rules (Göteborgs Stad, n.d.-d). These rules ensure that public entities remain objective and neutral towards potential suppliers and that the procurement process is transparent and understandable. The purpose of procurement laws is to ensure that contracting authorities use public funds in the best possible way and to provide suppliers with an opportunity to compete on equal terms. The legislation is founded on five key principles: non-discrimination, equal treatment, proportionality, transparency, and mutual recognition.

Each year, the City of Gothenburg spends 29.2 billion SEK on goods and services (Göteborgs stad, n.d.-e). The city's departments and companies independently manage their budgets and purchasing processes. Approximately 40 percent of all public contracts in Sweden are "framework agreements." These agreements are created when there is a recurring need for goods or services that are frequently purchased, large in scale, or of high value. Once a framework agreement is in place, authorities are not required to conduct new procurements each time they need those goods or services. Instead, they can place orders based on the existing agreement, which specifies what can be purchased and from whom during the contract period (typically lasting 2-4 years).

The City of Gothenburg is made up of around twenty departments and forty companies (Göteborgs stad, n.d). Each of these entities is responsible for its own finances and purchasing decisions. For suppliers, this means that Gothenburg is not a single customer, but rather a collection of many. Suppliers may hold separate contracts with different departments and companies simultaneously. These local agreements make up about 75 percent of the city's total procurement. In addition to the individual contracts with various departments and companies, there are also common agreements for the entire City of Gothenburg. These agreements are negotiated by the procurement department, acting as a purchasing center. Common agreements are made for areas with frequent or large-scale needs, such as food, office supplies, or furniture. Other municipalities and municipal associations in the Gothenburg region can also participate in these common agreements.

4

Results

In this sections findings from interviews with subcontractors and procurement profesionals is presented. The interviews were aimed to explore how the procurement process works and how the NIS2 and CER-directives are applied during this process. Moreover, the purpose is to get a better understanding of how these directives affect the procurement process and if there are identified challenges faced by subcontractors.

4.1 Awareness and Understanding of NIS2 and CER Directives

Within the Municipal Urban Environment Department (Stadsmiljöförvaltningen) the awareness and understanding of NIS2- and CER-directives comes in different layers. Departments like IT and information security units have a relatively higher level of awareness since they primarily handle cybersecurity risks as well as oversee digital infrastructure. Additionally, these departments have a solid understanding of how to follow the directives, including responsibilities such as incident reporting obligations and cybersecurity requirements. Moreover, the majority of the interviewees from the Municipal Urban Environment Department mentioned that not all departments are as aware of the directives and what they imply. Departments such as those not related to IT or risk management are usually unaware of what these directives are. While awareness of the directives is not consistent across all departments, the same participants noted that many, particularly those in leadership roles, are aware of their existence.

However, little has been done so far to actively implement them within the organization. This is particularly important for infrastructure, urban planning and public service. Furthermore, the same participants emphasized that due to the unfamiliarity of NIS2, suppliers find it difficult to know if they fall under its scope and what requirements they must meet. Participants from Göteborgs Spårvägar noted that they were aware of the directives and had some initial understanding of them. Nevertheless, they expressed uncertainty about how to move forward, as the legislation had not yet been finalized. This uncertainty was further reflected in the interview with the system developer from Infracontrol, a long-term supplier to

the municipality. Despite having provided services for over five years, they stated that they had not heard about the new directives and were unfamiliar with their content. Moreover, municipalities rely heavily on private actors for different types of services, making this inconsistency particularly problematic. The municipality's ability to comply with the directives also depends on these suppliers.

On the other hand, the security coordinator at Urban Environment Department spoke of how the department is already quite familiar with the NIS2 directive, having previously worked with its earlier version, NIS1. Although NIS2 has not yet been finalized into law, the department has been actively preparing for it. Compared to NIS1, the new directive has a much broader scope, covering the entire organization. The interviewee pointed out that delays in the Swedish legislative process have created a lot of uncertainty, making it difficult for the department to move forward with full implementation. As a result, while preparations are underway, they can't fully comply until the directive is legally in place. This uncertainty is also affecting suppliers, many of whom are unsure about the extent of their obligations under the upcoming rules. The main focus as a security coordinator is being responsible for CER-directive. The interviewee points out that the directive is not yet in force in Sweden. However, the municipality has assessed how it can affect the organisation and many requirements in the CER-directive already align with existing practises, particularly assessing risks and identifying critical operations. Moreover, various departments within the municipality such as traffic infrastructure, transport systems, and urban planning fall within the scope of the directive. There is a 13 page internal document that has been written to outline potential operational impacts, risk scenarios and identified gaps. Additionally, it includes a mapping of dependencies on external actors, services, and suppliers critical to both daily operations and emergencies.

4.2 Organizational Impacts of NIS2 and CER

Several interviewees, including the information security coordinator, the planning manager, and the security officer within the Urban Environment Department, stated that the NIS2 and CER directives have not yet had a significant practical impact, mainly because the legislation has not been fully implemented in Sweden. Nevertheless, these directives are expected to bring considerable changes to internal organizational processes. A recurring theme throughout the interviews was the need for security efforts to become more systematic and integrated across the entire organization, rather than being confined to individual departments.

Furthermore, several participants emphasized that achieving such integration requires active and sustained leadership engagement. The security manager at Göteborgs Spårvägar stressed that without leadership support, security work risks becoming reactive and short-term instead of proactive and sustainable. This perspective was echoed by the track infrastructure manager, who noted that although cybersecurity is already integrated into their operations, the Urban Environment Department needs to adopt a more structured approach by establishing routines,

providing clear instructions, and ensuring that their efforts can be monitored and evaluated by the relevant authorities. Furthermore, the security coordinator from the Urban Environment Department highlighted that "Security work must not be isolated, but integrated into daily management and development. Security should be seen as a quality criterion, not a burden."

Risk management and preparedness have emerged as key areas for adaptation. However, several interviewees pointed out that many departments already carry out extensive work in these fields. The planning manager for signal operations explained that their team routinely conducts both risk and gap analyses to identify vulnerabilities and determine necessary actions. Consequently, the new directives are not expected to drastically alter their current practices, but rather to reinforce and formalize existing routines.

Education was further identified as a critical factor. One respondent, the IT Procurement Officer, explained that they are responsible for educating others within the Urban Environment Department, yet acknowledged that no concrete training plans had been developed at the time of the interview. Similarly, the track infrastructure manager pointed to the lack of formal training, stating that "There has been no training. Most of it is self-study and we wait for updates. But it is our responsibility to ensure that those who need competence development actually receive it." Additionally, participants from both Göteborgs Spårvägar and the municipality mentioned plans to introduce comprehensive training programs aimed at all employees. These initiatives are intended not only to raise general awareness of risks but also to emphasize the importance of information protection across all organizational levels.

4.3 Integration of NIS2 and CER Directives into Procurement and Supplier Management

Within the municipality, the integration of NIS2- and CER-directives are very limited due to the pending legislative process. During an interview with an IT officer for procurement from the Urban Environment Department, it was mentioned that these directive do not play a formal role in the procurement process since it has not been transposed into Swedish law. However, there is an awareness and some preliminary actions such as stricter incident reporting timelines, may be embedded into future procurement demands. The interviewee emphasized that the existing procurement process already includes general information security requirements. Therefore, after the legislative enforcement of the directives, there will presumably not be a drastic shift in the contracts but rather an introduction of new expectations. Additionally, the participant noted that it will be very challenging to ensure that suppliers, particularly smaller firms, are capable of meeting new cybersecurity and risk management expectations. The procurement process will therefore need more proactive communication with suppliers ahead of tenders. At the Urban Environment Department, the Track Infrastructure Manager explained that their procurement practices

already include a clause in all new contracts requiring suppliers to prepare for the implementation of NIS2 and CER. Although the wording of this clause remains somewhat vague, it nonetheless creates a binding contractual obligation for suppliers.

The current contracts are not completely designed to support the directives however they are not obstructing them either. According to the security coordinator, another complication is that current contracts don't yet reflect the requirements of NIS2 and CER. This then makes the procurement process more difficult. That said, some suppliers, especially those in IT and those already operating within the EU, are more aware of cybersecurity and data protection responsibilities, thanks to experience with GDPR. Moreover, one recommendation given by the participant is to define roles related to information ownership and risk management within the organization.

A shift in how security requirements are handled was also highlighted. The IT Procurement Officer stressed the importance of establishing clear, specific, and binding security requirements that are well-founded and practical. The Crisis and Preparedness Manager added that classifying information and determining appropriate protection levels are essential steps for translating these regulatory directives into actionable procurement documents. According to the Information Security Coordinator the supplier requirements should be managed in layers, starting with external protections and gradually moving inward toward the most critical systems.

4.4 Challenges in Implementing NIS2 and CER Directives

The interviewees described a broad range of challenges in the implementation of the NIS2 and CER directives. These challenges primarily concerned legal uncertainty, limited competence and resources, internal coordination, procurement difficulties, and issues related to suppliers. One of the most commonly raised concerns was the absence of clear legal guidance. Since national legislation has not yet been finalized, many participants expressed uncertainty about what specific actions to take. Consequently, several interviewees noted that their organizations have adopted a wait-and-see approach, which has delayed concrete measures. Furthermore, the complexity of the regulatory landscape was repeatedly emphasized. According to the security coordinator at the Urban Environment Department, their organization is expected to comply with several frameworks issued by different authorities, which sometimes present conflicting guidance and contribute to confusion.

In addition, competence gaps and difficulties in interpreting the directives were frequently highlighted. Several interviewees described challenges in understanding the broad and general legal language and in translating it into specific, practical steps for their systems. Limited resources also emerged as a recurring theme. Many participants pointed out that information security is often treated as a secondary responsibility within their organizations, which has led to fragmented attention and

inconsistent prioritization. The planning manager explained that it was particularly difficult to apply general requirements to their technical systems in a meaningful and accurate way. Moreover, internal responsibility and coordination were described as unclear, especially in municipal contexts where multiple departments share systems but fall under different administrations. The planning manager remarked that this structural fragmentation makes it difficult to establish who is ultimately responsible for ensuring compliance across organizational boundaries.

Leadership involvement was considered essential for the successful long-term implementation of the directives. While initial interest in the directives was described as strong by the majority of the interviewees, the information security coordinator compared the situation to a "ketchup effect," where attention builds quickly but then fades. Concerns were raised about whether leadership commitment would be sustained over time. The security manager at Göteborgs Spårvägar emphasized the importance of continuity and long-term investment, describing the implementation process as a substantial undertaking that requires both time and financial resources. Moreover, procurement was identified as another key area of difficulty. The procurement officer stressed the importance of setting clear requirements at the beginning of the procurement process. A specific challenge involved long-term contracts signed before the directives came into effect. These contracts may remain valid for several years, and according to the procurement officer, suppliers bound by them are not required to comply with the new directives, which creates potential vulnerabilities within the system.

Supplier capacity to meet the new requirements was also questioned. The information security coordinator noted that only a limited number of suppliers may be able to meet the stricter cybersecurity demands. Monitoring suppliers was described as particularly challenging, especially in cases involving remote access or subcontracted services, which complicate risk assessment and control. According to the coordinator from Göteborgs Spårvägar, some subcontractors have already indicated that the upcoming requirements could lead to delays. This was described as a concern, especially in light of the long-standing relationships with many suppliers, which may require additional time and support to adapt to the updated expectations. Finally, psychological resistance to change was mentioned by several interviewees as a more subtle but still significant barrier. Some participants observed that uncertainty and a lack of confidence in interpreting the directives made staff hesitant to engage in discussions or initiate preparatory actions, which has further delayed organizational readiness.

5

Discussion

This chapter reflects on the challenges and opportunities identified through interviews with municipal staff and suppliers regarding the implementation of the NIS2 and CER directives. Several key themes emerged, relating to organizational structures, knowledge gaps, supplier relations, procurement processes, information sensitivity, and the ongoing nature of compliance. These aspects are discussed below to provide a comprehensive understanding of the practical implications and areas for future focus.

In the context of public sector operations and procurement processes, the NIS2 and CER directives introduce a range of operational and structural challenges. Interviews with professionals from both the municipality and its suppliers revealed recurring themes related to organizational capacity, preparedness, and governance, both internally and across external partnerships. A key issue identified is the lack of clear internal governance structures, which significantly affects the ability to implement the directives effectively. Many interviewees described roles and responsibilities around security and risk management as vague, with uncertainty about who is accountable for compliance decisions and risk acceptance. This lack of clarity hinders coordination across departments and undermines consistent implementation. These findings reflect the broader concerns raised by Mikac (2023) and Rehnstam et al. (2025), who argue that public sector organizations often delay action due to the complexity of the directives and limited national guidance. In this context, vague internal structures further contribute to hesitation and fragmented progress.

Another major barrier to effective implementation is the limited availability of formal education and structured training. Most participants had received little or no instruction regarding the directives, and much of the current knowledge relies on informal conversations or self-directed learning. This knowledge gap contributes to organizational uncertainty and increases the risk of misinterpretation. During the interview process, several individuals expressed reluctance to participate due to their limited understanding of NIS2 and CER. Some declined entirely, while others avoided the subject rather than admit to uncertainty. This widespread hesitation suggests a deeper discomfort around the directives and illustrates how a lack of internal transparency and structured knowledge-sharing can hinder preparedness efforts. The study further revealed that awareness of the directives is highly uneven across roles and departments. Employees working in IT, security, or leadership roles

generally showed a solid grasp of the directives, while those outside these areas often had little or no awareness. For instance, a representative from Infracontrol admitted being unaware of the directives altogether. This reinforces the notion of uneven understanding within and across organizations and indicates a need for broader communication strategies. Sadeghi et al. (2023) describe this phenomenon as limited absorptive capacity the inability of an organization to absorb, interpret, and act on new knowledge which is especially detrimental when responding to emerging security requirements.

Concerns about future implementation extend beyond internal structures. One interviewee noted that some suppliers had already raised worries about potential delays in their service delivery once the directives come into force in Sweden. This adds another layer of complexity, as there is a risk that some suppliers may not be prepared to meet the new requirements within the required timeframe. If certain vendors are unable to comply, municipalities may have to seek alternative suppliers to ensure service continuity. A particular challenge lies with existing long-term contracts established before the NIS2 and CER directives came into effect. These agreements often lack provisions to address the new security requirements, creating compliance gaps once the directives become legally binding. Because these contracts remain valid for their full duration, both the municipality and suppliers may struggle to update terms and conditions quickly. This can lead to breaches in the supply chain, with suppliers bound by outdated contracts facing difficulties in fulfilling new obligations, potentially causing service disruptions or expensive renegotiations. However, replacing long-term partners is not simple. Such relationships are typically built on trust, shared knowledge, and years of cooperation. Terminating contracts due to non-compliance risks technical and logistical disruptions, especially in sectors like public transportation where system familiarity is vital. Moreover, pushing for immediate compliance may alienate suppliers who, with proper support and a phased transition plan, could successfully adapt. This highlights the importance of proactive communication and gradual compliance strategies to maintain continuity while meeting regulatory demands.

Beyond these operational concerns, the new directives also pose significant challenges for small and medium-sized enterprises (SMEs). With cybersecurity and data protection now embedded as mandatory components in public procurement, many SMEs face the risk of exclusion. Due to limited financial and technical resources, smaller suppliers may find it difficult to meet new certification or infrastructure requirements. Several interviewees voiced concern that these expectations could unintentionally disadvantage SMEs, especially in larger municipalities like Gothenburg, where procurement systems are more complex. This is consistent with findings by Jan et al. (2023), who note that SMEs are often overwhelmed by advanced compliance demands, particularly when lacking dedicated cybersecurity personnel. ENISA (2022) also emphasizes that even when SMEs are not directly regulated by NIS2, they are still affected indirectly through flow-down requirements from their clients. If procurement strategies are not adapted to accommodate different capacities, municipalities risk reducing supplier diversity and weakening the overall resilience of their infrastructure.

Regarding the procurement process itself, most participants felt that the existing requirements generally aligned well with the new directives but still required some adjustments. For example, they requested clearer guidance and more detailed information about what the directives mean for suppliers. It was also considered crucial to have binding regulations in place, as many suppliers might otherwise exploit loopholes in contracts. To address this, the use of a common contract template was seen as necessary to provide a consistent foundation.

Another critical area raised during the study concerns the handling of sensitive information. Although the municipality does not deal with classified defense data, several interviewees noted that it does manage operationally sensitive information such as signaling layouts, maintenance routines, and technical infrastructure details. Under NIS2 and CER, this type of data gains new importance in ensuring security and preventing malicious interference. This raises important questions what kind of information should be considered sensitive? How should it be handled, shared, and protected in procurement contexts? And how can public organizations maintain necessary transparency without jeopardizing operational security?

These questions become particularly relevant in light of the municipality's responsibility for critical infrastructure. While transparency is essential for fair competition and accountability in public procurement, too much openness can pose risks if sensitive operational data becomes publicly accessible. Hellberg (2023) discusses this tension in the context of defense procurement, noting the difficulty in balancing openness with confidentiality. He argues that one of the key challenges is defining what qualifies as sensitive information, and that the lack of a clear classification framework leaves procurement staff and suppliers to make individual judgments. This increases the likelihood of both inconsistency and underprotection. In the case of NIS2 and CER, failing to establish clear confidentiality routines could create significant vulnerabilities in the supply chain.

Finally, a recurring theme throughout the interviews was the importance of maintaining compliance over time. Both NIS2 and CER are not static requirements; they call for continuous engagement, including regular risk assessments, updates to internal procedures, and ongoing audits. This is particularly important in systems like public transport, where operational reliability and public safety are directly linked. Implementing the directives requires a shift from viewing cybersecurity as a one-off technical fix to embracing it as an ongoing organizational responsibility. Several respondents emphasized that strong leadership is key to embedding these practices into daily routines. Without it, there is a risk that organizations will revert to reactive approaches once the initial implementation push subsides. This insight aligns with the work of Lemnitzer and Prockl (2023), who argue that sustainable implementation depends on long-term leadership commitment and a culture of shared responsibility across the organization.

6

Recommendations

This chapter offers several suggestions aimed at supporting Gothenburg Municipality in effectively preparing for and implementing the NIS2 and CER directives. These recommendations may also be relevant and useful for other organizations. The chapter concludes with proposals for future research within this field.

6.1 Key Recommendations for Effective Directive Implementation

Establish structured awareness and training initiatives

Education regarding the directives should be implemented promptly for all affected departments and should not rely solely on self-directed learning, as this often leads to gaps in knowledge. Short information sessions, clear written guidelines, and internal newsletters can enhance awareness across the organization. Training programs should be customized to the specific roles within the municipality and extended to relevant suppliers to ensure a shared understanding of requirements.

Revise procurement templates and criteria

A key recommendation is to integrate explicit security requirements early in the procurement process by embedding them into templates and tender criteria. This aligns with ENISA's (2022) guidelines, which emphasize the importance of addressing security concerns at the procurement stage. The municipality's ongoing efforts in this area should be prioritized and further developed.

Adapt requirements according to service criticality

To avoid unintentionally excluding small and medium-sized enterprises (SMEs), the municipality should apply differentiated security requirements based on the criticality of the service. For highly critical systems, such as signaling, full compliance should be mandated immediately. For medium-critical services, such as IT maintenance, transitional timelines could be applied, while low-critical services may continue under existing procedures but with regular reviews.

Introduce future-proof contract clauses

New contracts should include provisions that allow for security requirements to be updated following the transposition of the directives into Swedish law. For existing long-term agreements, the municipality should consider incorporating "trigger clauses" in future contracts. Such clauses would obligate suppliers to update their security plans within a specified timeframe after the directives come into force or enable contractual adjustments, facilitating a smoother transition for both parties.

Develop policies for information classification and protection

Operational data should be formally classified based on risk assessments. Procurement contracts should clearly define standards for data encryption, access control, and personnel vetting. These measures will increase trust and legal clarity among supplier relationships and contribute to a more resilient operational ecosystem.

Coordinate compliance with existing regulations

To streamline implementation efforts, the municipality should map overlaps between NIS2, CER, and existing regulatory frameworks such as GDPR. Identifying areas where requirements are already fulfilled can reduce redundant work and help harmonize internal policies.

Build on existing internal strengths

Departments that have already established robust security practices should document and share these as internal best-practice models. Communicating these success stories can reduce resistance to change and accelerate adoption of the directives across the organization.

6.2 Future research

While this study offers valuable insights into the current challenges and opportunities related to the implementation of the NIS2 and CER directives, several areas require further exploration. One important avenue for future research is to conduct longitudinal studies that follow municipalities and suppliers over time. These studies could examine how compliance strategies evolve, how effective training programs are in the long term, and how governance structures adapt to meet regulatory demands. Another key area involves understanding how small and medium-sized enterprises are affected by the new cybersecurity and resilience requirements. This includes identifying practical barriers they face in procurement processes and evaluating which forms of support, such as targeted funding or simplified compliance frameworks, might enable broader participation without compromising security. In addition, future research could explore how leadership and organizational culture influence the successful integration of continuous cybersecurity responsibilities. This might involve studying how different leadership styles and change management strategies affect employee engagement and institutional commitment. Finally, there is an in-

creasing need to examine how digital technologies such as artificial intelligence, real-time monitoring, and predictive analytics can support more dynamic and proactive compliance with the directives, particularly in complex public infrastructure systems.

7

Conclusion

This study set out to explore how procurement and supplier relationships can be organized to ensure that the tramway system within the Municipality of Gothenburg complies with the NIS2 and CER directives. Using a qualitative case study approach based on interviews with municipal employees, suppliers, and security coordinators, the research identified a range of challenges, knowledge gaps, and opportunities linked to the implementation of these regulatory frameworks. The findings show that while awareness of the directives is gradually increasing within certain departments, particularly those working with IT and information security, it remains inconsistent across the broader organization. Many suppliers are uncertain about their obligations, partly due to delays in national legislation and partly due to limited internal communication and training. This highlights the need for improved knowledge-sharing and for ensuring that suppliers are actively informed and engaged in the compliance process.

In response to the research question, which asked how procurement and supplier relationships can be organized to ensure compliance with NIS2 and CER, the study concludes that clear and binding security requirements must be introduced early in the procurement process. These requirements should be embedded in contract structures that allow for future updates and tailored to reflect the criticality of the services provided. Strengthening supplier collaboration, offering transitional support, and enhancing contract flexibility are essential to manage compliance effectively without compromising service delivery. The study also emphasizes the need for consistent classification of sensitive operational data, improved coordination between departments, and stronger leadership engagement to ensure that cybersecurity and resilience are fully integrated into daily operations. Overall, this thesis contributes to a deeper understanding of how public sector organizations can prepare for and respond to new cybersecurity regulations. Although the research is based on a single case, the lessons drawn and recommendations proposed may offer guidance to other municipalities and public entities working to secure their critical infrastructure in an increasingly complex risk environment.

References

DeJonckheere, M., & Vaughn, L. M. (2019). Semi-structured interviewing in primary care research: A balance of relationship and rigour. In *Family Medicine and Community Health,* 7(2), e000057. https://doi.org/10.1136/fmch-2018-000057

Dokuchaev, V. A., & Maklachkova, V. V. (2023). Cybersecurity Impact on the Transport Security. In *2023 International Conference on Engineering Management of Communication and Technology (EMCTECH)* (pp. 1–6). IEEE. https://doi.org/10.1109/EMCTECH58502.2023.10297009

Dong, B.-X., Shan, M., & Hwang, B.-G. (2022). Simulation of transportation infrastructures resilience: a comprehensive review. *Environmental Science and Pollution Research*, 29(9), 12965–12983. https://doi.org/10.1007/s11356-021-18033-w

Elsner, M., Atkinson, G., & Zahidi, S. (2025, January). *Global Risks Report 2025*. World Economic Forum.

ENISA. (2023, June). *Good Practices for Supply Chain Cybersecurity*. ENISA Reports.

European Union. (2024). *EU:s prioriteringar för 2024–2029*. European Union.

Göteborgs stad. (n.d.-a). *Om kommunens organisation*. Göteborgs stad.

Göteborgs stad. (n.d.-b). *Spårvagnstrafiken i Göteborg och Mölndal*. Göteborgs stad.

Göteborgs stad. (n.d.-c). *Verksamheter inom stadsmiljöförvaltningen*. Göteborgs stad.

Göteborgs Stad. (n.d.-d). *Lagar och regler inom upphandling*. Göteborgs Stad.

Göteborgs Stad. (n.d.-e). *Så fungerar inköp och upphandling i Göteborgs Stad*. Göteborgs Stad.

Hellberg, R. (2023, November). Swedish public procurement and the defence industry: obstacles and opportunities. *Journal of Defense Analytics and Logistics*, 7(2), 103–137. https://doi.org/10.1108/JDAL-12-2022-0015

Hellberg, R., & Lundmark, M. (2025, January). Transformation in European Defence Supply Chains as Ukraine Conflict Fuels Demand. *Scandinavian Journal of Military Studies*, 8(1), 17–39. https://doi.org/10.31374/sjms.303

Kelliher, F. (2022, October). Qualitative case study research methods in supply chain management. In *Handbook of Research Methods for Supply Chain Management* (pp. 125–148). Edward Elgar Publishing. https://doi.org/10.4337/9781788975865.00013

Lim, W. M. (2025, May). What Is Qualitative Research? An Overview and Guidelines. *Australasian Marketing Journal*, 33(2), 199–229. https://doi.org/10.1177/14413582241264619

Lemnitzer, J. M., & Prockl, G. (2023). The NIS 2 Directive – Where Cyber Risk meets Supply Chain Management.

Mikac, R. (2023). Protection of the EU's Critical Infrastructures: Results and Challenges. *Applied Cybersecurity & Internet Governance*, 2(1), 1–5.

Myndigheten för samhällsskydd och beredskap. (2012). *Har du koll? Säkerhetspolitik. Faktafördjupning*. MSB.

Myndigheten för samhällsskydd och beredskap. (2025, March). EU och arbetet med att stärka motståndskraften i samhällsviktig verksamhet. MSB.

National Cyber Security Centre. (n.d.). *NIS 2: A Quick Reference Guide*. National Cyber Security Centre.

Nweke, L. O., & Wolthusen, S. (2020, May). Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure Protection. In *2020 12th International Conference on Cyber Conflict (CyCon)* (pp. 63–78). IEEE. https://doi.org/10.23919/CyCon49761.2020.9131721

Raponi, S., Caprolu, M., & Di Pietro, R. (2021). Beyond SolarWinds: The Systemic Risks of Critical Infrastructures, State of Play, and Future Directions. *ITASEC*, 21, 7–9.

Regeringskansliet. (2024a). Nya regler om cybersäkerhet. *Regeringskansliet*.

Regeringskansliet. (2024b). Motståndskraft i samhällsviktiga tjänster. *Regeringskansliet*.

Rehnstam, E., Winquist, W., & Hacks, S. (2025). NIS2 Directive in Sweden: A Report on the Readiness of Swedish Critical Infrastructure. In *Springer Nature Switzerland* (pp. 176–195). https://doi.org/10.1007/978-3-031-79007-2_10

Sadeghi R., K., Azadegan, A., & Ojha, D. (2023, May). A path to build supply chain cyber-resilience through absorptive capacity and visibility: Two empirical studies. *Industrial Marketing Management*, 111, 202–215. https://doi.org/10.1016/j.indmarman.2023.04.001

Serdar, M. Z., Koç, M., & Al-Ghamdi, S. G. (2022, January). Urban Transportation Networks Resilience: Indicators, Disturbances, and Assessment Methods. *Sustainable Cities and Society*, 76, 103452. https://doi.org/10.1016/j.scs.2021.103452

Säkerhetspolisen. (2023). Säkerhetsskyddsavtal vid upphandlingar och samarbeten. SÄPO.

Sveriges Kommuner och Regioner. (2024, October). NIS-direktivet, NIS2 och CER-direktivet. Sveriges Kommuner och Regioner.

University of Oslo. (2023). Complying with Supply Chain Security Requirements under the NIS-2 Directive. University of Oslo.

Van't Schip, M. (2024). View of The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things. *European Journal of Law and Technology*, 15(1).

A

Appendix 1

Appendix 1: Interview Questions

Role and Background

1. Can you briefly describe your role and responsibilities within your department or organization?

Familiarity with NIS2 and CER

2. How familiar are you with the NIS2 and CER directives, and what role do these directives play in your daily work?

3. Have you received any specific training or support to understand and implement these directives?

Procurement and Impact

4. How have the NIS2 and CER directives affected your organization's procurement process?

5. From a crisis preparedness perspective, have you noticed any concrete changes related to these directives?

Crisis Preparedness and Integration of the Directives

6. How do you integrate the NIS2 and CER directives into your crisis management strategies?

7. How do these directives impact the procurement of tools or services for crisis preparedness and management?

8. What role do data protection and cybersecurity play in the crisis management systems you work with?

9. How do you ensure that your suppliers provide solutions that comply with the NIS2 directive and meet your preparedness requirements?

10. What specific challenges do you see in integrating these directives into procurement contracts, especially with suppliers who may not be fully familiar with them?

Risk Management and Cooperation

11. How do you manage risks and ensure that critical parts of your operations continue during disruptions?

12. How do you collaborate with authorities or other companies regarding the NIS2 and CER directives?

13. Are there particular types of events or scenarios that you focus on more heavily in your preparedness work?

14. Who is responsible for reporting incidents, and how quickly must this be done?

15. What do you see as the biggest difference between working under the new directives compared to previous regulations or frameworks?

Improvements and Advice

16. What improvements or changes do you think should be made to the procurement process to better align it with the requirements of NIS2 and CER?

17. What advice would you give to other actors who are struggling to integrate these directives into their procurement processes?

18. Do you think the current procurement process is effective in ensuring compliance with NIS2 and CER, or are there areas that need improvement?

Closing

19. Is there anything else you would like to add?

DEPARTMENT OF SOME SUBJECT OR TECHNOLOGY
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden
www.chalmers.se

CHALMERS
UNIVERSITY OF TECHNOLOGY