Compliance Standards and Frameworks and Its Implications on Cybersecurity: A NIS2 Study Within the Swedish Automotive Industries

Adenike Adesina, Elias Seid, Fredrik Blix and Oliver Popov
Department of Computer and Systems Sciences, Stockholm University, Sweden

Keywords: Cybersecurity, EU Regulations, NIS2 Directive, Automotive Industry, Compliance, Standards, Cybersecurity Frameworks, Complexities, Organisational Preparedness.

Abstract: Cybersecurity standards and regulations are pivotal in guiding organizations toward mitigating cyber risks and enhancing their overall security posture. The European Union's NIS2 Directive, which introduces stringent and comprehensive security requirements, exemplifies a Current regulatory framework designed to address evolving cyber threats. This study critically examines the regulatory, governance, cybersecurity, and compliance challenges introduced by NIS2 within the Swedish automotive industry. It further explores the strategic integration of NIS2 with existing regulatory frameworks to streamline compliance approaches and foster long-term resilience. The findings reveal the increasing complexity and financial implications of compliance, while also identifying significant opportunities to bolster cybersecurity resilience. This paper underscores the necessity for organizations to adopt proactive and adaptive strategies in response to the dynamic European regulatory landscape. While the focus is on the Swedish automotive sector, the study provides valuable insights that may inform future research into the broader implications of NIS2 across diverse industries and regions within the European Union.

1 INTRODUCTION

Organisations are constantly exposed to cyber threats due to increased digitization and interconnectivity. These complexities have underpinned the need to introduce measures to protect individuals and organisations in today's complex digital world. Over time, there have been legislative interventions and published standards at both international and national levels to mitigate the effects of unceasing threats to infrastructure and information security. GDPR, ISO Standards 1, NIST 2, Network and Information Systems (NIS) Directive and most recently, NIS2 are some of the building blocks for practices to achieve cybersecurity. Knowledge of these frameworks not only defines or highlights certain security expectations and obligations for organisations, but some also prescribe punitive measures that guarantee strict compliance when in defiance. It goes without saying that compliance frameworks are already in existence, and there will still be more in the coming years. As industries will be affected by some of these regulations, especially the NIS2 Directive, cybersecurity will no longer be an afterthought or a reactionary measure in risk management. Hence, this study aims to examine the recent EU cybersecurity regulatory framework, mapping its interplay with other related frameworks to determine its implications for achieving cybersecurity within the automotive industry in Sweden.

Motivation. Cyber threats vary. They are unceasing and relentless in this era of increased digitization and interconnectedness. Some industries are more prone to the impact of cyber threats due to an increasing level of dependency on networks. For instance, the attack vector has widened in the automotive sector as industries constantly face ransomware, data theft and cyber incidents (Upstream, 2023). Even their supply chain has not been spared (Hill, 2023). These threats are constantly persistent and evolving and are poised to disrupt operational functions, and regulations are only reactionary and playing catch up.

However, given the new regulatory penchant of the EU in furtherance of its accord to securing Europe digitally and economically, there is an ever-increasing cybersecurity compliance requirement for companies in the EU (Lucini, 2023). These legislative exercises not only underpin the importance of legislation in decreasing cyber-attacks (Hasan et al., 2021) but also reveal the government's level of awareness and commitment to combat cyber-attacks. Consequently, this topic aligns with the current EU legislative act, as organisations will be affected by the new NIS2 Directive. Hence, this project aims to analyse the EU legislative framework and its intersection with other

Adesina, A., Seid, E., Blix, F. and Popov, O.
Compliance Standards and Frameworks and Its Implications on Cybersecurity: A NIS2 Study Within the Swedish Automotive Industries.
DOI: 10.5220/0013321200003899

In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 1*, pages 367-376
ISBN: 978-989-758-735-1; ISSN: 2184-4356

compliance standards in achieving cybersecurity requirements.

1.1 Regulations, Standards, and Guidelines

Regulations constitute a greater challenge as businesses and nations navigate a web of evolving regulations, standards, and guidelines, which can significantly impact organisational response (Kianpour & Raza, 2024). The Network and Information Security (NIS) Directive represents the first EU-wide legislation focused on cybersecurity. Its primary goal was to establish a consistent and robust level of cybersecurity across all EU Member States 3. However, despite its intentions, implementing the original NIS Directive encountered challenges, leading to a need for a review of the Directive (Markopoulou & Papakonstantinou, 2021). With the new NIS2 regulatory regime in place with imminent mandatory transposition requirements into national laws by member states, it has become pivotal to explore the regulatory gaps that may be experienced by one of the sectors. This new legal framework poses new regulatory risks due to uncertainties and complexities that new regulations have been identified to instigate (Kianpour & Raza, 2024). Over time, studies have explored the usefulness and applicability of frameworks constantly being published (Teodoro et al., 2015) (Taherdoost, 2022). Gisladottir et al (2017) explored the impact of cybersecurity regulations on organisations and employees and provided a framework for systematically evaluating rules, risk, and resilience of cyber systems incorporating behavioural science.

Even though regulations as a form of legislative interventions are valuable indicators and predictors of an organisation's readiness to combat cyber-attacks (Teodoro et al., 2015), there is a lack of awareness of these regulations (Hasan et al., 2021) and how to implement the measures required by any cybersecurity framework is an impediment to realizing the ambitious goals of any legislative piece. A survey also identified that rules or standards related to cybersecurity are almost unknown in the business world (Syafrizal et al., 2022). This position is further stressed in a study by (Sirur et al., 2018), where interviewees agreed that GDPR was a step towards more thoughtful cybersecurity practices. However, organisations struggled to understand how to comply and what technical and organisational security requirements are necessary.

However, the success of CS depends on how readily an organisation facilitates the implementation of regulatory requirements (Marotta & Madnick, 2020) and (Kianpour & Raza, 2024) explains that businesses are actively seeking to understand and adhere to the stipulations of the updated NIS2 Directive to ensure that their operations remain uninterrupted, safeguard their reputation, and avoid stringent penalties.

The automotive industry is a vital sector 4 (Karamoozian et al., 2024) that faces heightened cybersecurity risks as the digital landscape evolves 5 (Kalogeraki & Polemi, 2024). Lucini (2023) identified that many operators exempted by the previous NIS Directive could now face new compliance challenges when operating in Europe. Organisational preparedness, adaptability, and agility for the new NIS2 regulatory framework are now considered necessary in safeguarding infrastructure assets and avoiding regulatory alties. Despite the rising interest in the NIS2 legislative framework (Kianpour & Raza, 2024), little perspective has been known about how this new legislation is perceived within the industry and the trails that can be used to determine this domain's state of readiness regarding its implications and implementation outlook. and cybersecurity regulations as multifaceted and complex (Babikian, 2023). So far, no research has been carried out on the implications of the revised NIS Directive and the influence of other compliance standards and frameworks on achieving cybersecurity requirements within the automotive sector in Sweden. Existing studies primarily focus on various standards and regulations applicable to different entities within the EU (Kalogeraki & Polemi, 2024; Syafrizal et al., 2020).

Though (Lucini, 2023) study was about NIS2 within the EU, its scope was broad. Still, no study has examined the specific implications of the requirements of the new NIS Directive in interplay with frameworks and standards for achieving CS obligations within the automotive industry in Sweden. Since there is a lack of empirical data to elicit and analyse the perspectives of automotive professionals on the implications of regulatory changes and how extant practices within the industry also influence compliance, hence this study. Since there is limited understanding, particularly as to whether automotive industries are regulatory aware of their scope under NIS2 and how they navigate the evolving cybersecurity landscape under the EU NIS2 Directive, research is needed to explore this.

The Objective of the Study. With the increased cybersecurity risks posed by cybercriminals and adversaries, it has become imperative for organisations to increase their awareness of the change in the cybersecurity landscape and respond effectively to change (Lee, 2021). This research aims to explore the perception of cybersecurity professionals within the automo-

tive sector in readiness for NIS2 mandatory propositions, as it is not a matter of choice whether to implement NIS2; it is a matter of when. The study examines the cybersecurity requirements in preparation for the imminent compliance expectations. This research aims to answer this question:

RQ: Does the new EU Directive have any implications on cybersecurity compliance within the Swedish automotive sector?

2 RESEARCH BASELINE

2.1 Digitization and Its Challenges

The need for comprehensive IT security standards and regulations to enhance cybersecurity is widely recognized. Fumy (2004) emphasized the critical roles of governments and the private sector in developing and promoting these standards. Cybersecurity regulations, as highlighted by Srinivas, Das, and Kumar (2019), compel organizations to safeguard their systems and information against cyber-attacks. Research underscores the importance of government legislation in reducing cyber threats, urging compliance to enhance preparedness and incident handling (Hasan et al., 2021). Public demand for stricter regulations and heightened awareness of privacy have spurred proactive cybersecurity policies (Kianpour & Raza, 2024). A lack of stringent regulations enables companies to sidestep cybersecurity laws (Wall et al., 2016). Furthermore, organizations often underinvest in cybersecurity, prioritizing profits over robust security measures (Radziwill & Benton, 2017; European Commission, 2020). Cyber insecurity is now a major global risk (World Economic Forum, 2024), necessitating multidimensional solutions beyond technical measures (Gercke, 2013). Legal tools have proven essential in managing cyber risks (Kasper & Antonov, 2019).

Governments worldwide are focusing on reducing cyber risks through regulations (Meltzer, 2020; Kuhn, 2018). The evolving regulatory landscape reflects a response to emerging threats, compelling organizations to adopt stringent cybersecurity measures (Srinivas et al., 2019). For instance, the automotive sector faces unique cybersecurity challenges due to the rise of interconnected vehicles and complex supply chains, necessitating enhanced security practices (Fernandez de Arroyabe et al., 2023; Khan, 2019). In Europe, the NIS2 Directive expands on previous legislation to ensure a high level of cybersecurity across member states. It broadens its scope to include critical and important entities, introducing stricter security requirements and comprehensive risk management measures (Lucini, 2023). Similarly, the GDPR aims to curb personal data misuse, promoting more deliberate cybersecurity practices (Sirur et al., 2018). The Critical Entities Resilience (CER) Directive further strengthens infrastructure resilience across ten key sectors, mandating proportional technical, security, and organizational measures by 2026. These developments reflect a global shift toward robust cybersecurity regulations to address increasingly complex threats and ensure organizational readiness.

In response to the growing cyber threats against organizations, cybersecurity frameworks provide essential practices and standards to strengthen cyber resilience and minimize risks (Srinivas et al., 2019). While legislative frameworks like NIS2 prescribe broad cybersecurity requirements, industry-specific regulations such as UNECE R155/R156 mandate cyber risk assessments in the automotive sector. Frameworks like ISO/SAE 21434:2021 focus on end-to-end cyber-risk management within road vehicle engineering (Taherdoost, 2022), while the NIST Cybersecurity Framework, widely adopted for its flexibility, emphasizes risk management, resource prioritization, and a comprehensive cybersecurity strategy (Scofield, 2016). Similarly, ISO 27001 provides a holistic approach to information security, integrating risk management and operational excellence across all sectors. These frameworks collectively guide organizations in navigating complex regulatory requirements and bolstering their cybersecurity posture through standardized practices and integrative approaches.

2.2 Regulatory Risks and Compliance Burden

Kianpour and Raza (2024) highlighted the hidden risks and challenges posed by cybersecurity regulations, including complexities and uncertainties that can disrupt organizational planning, strain resources, and create competitive disadvantages. These risks, categorized as regulatory, compliance, cybersecurity, and governance, often intersect and collectively impact businesses. Regulatory risks arise from changes in legal frameworks, compliance risks involve penalties for non-adherence, cybersecurity risks pertain to vulnerabilities in digital infrastructure, and governance risks stem from ineffective leadership and decision-making (Kianpour & Raza, 2024). For instance, the transition from the NIS Directive to NIS2 introduces new obligations and procedural terms, requiring businesses to adapt or face strategic disruptions (Lucini, 2023). While effective cybersecurity readiness enhances organizational security, improves

performance, and boosts customer trust (Hasan et al., 2021), rapid regulatory changes complicate management processes (Lee, 2021). Organizations must navigate a blend of regulations, standards, and governance frameworks, tailored to their industry, geography, and products, to implement effective cybersecurity measures and limit legal exposure as these frameworks evolve (Lucini, 2023).

3 METHODOLOGY

This study adopted a case study approach to assess the readiness of automotive companies for the new EU cybersecurity legal framework (NIS2). A case study method was selected for its ability to provide an in-depth examination of practices and implications within a specific context, making it particularly suitable for evaluating regulatory readiness (Denscombe, 2010; Edgar & Manz, 2017). This method allowed the use of multiple data sources, such as questionnaires, document reviews, and semi-structured interviews, to gather empirical evidence and develop a comprehensive understanding of the phenomenon. Alternative research strategies like experiments, ethnography, and phenomenology were considered but deemed less suitable as the study focuses on organizational readiness within a natural setting rather than artificial or cultural contexts (Johannesson & Perjons Erik, 2014; Denscombe, 2010).

Data were collected through a combination of online questionnaires and semi-structured interviews, providing flexibility and depth to address the research questions (Denscombe, 2010). Questionnaires allowed efficient data collection across geographic locations, while semi-structured interviews provided detailed insights from IT managers, security officers, and compliance officers with knowledge of NIS2 readiness. Purposive and snowball sampling methods ensured responses from relevant stakeholders and referrals for additional participants. Other methods, like focus groups and direct observations, were excluded as they were less aligned with the study's objectives. While quantitative and qualitative data sources were considered valuable, the study prioritized methods that balanced depth with feasibility (Myers, 2013).

Thematic analysis was employed to analyze qualitative data, following Braun and Clarke's (2006) systematic approach. Audio-recorded interviews were transcribed, and the data were reviewed multiple times to identify patterns and key ideas. Preliminary codes were developed, refined, and grouped into subthemes, which were further organized into overarching themes. A thematic map was created to visualize connections between themes, and these were finalized to represent the data accurately. This approach ensured a coherent narrative that linked findings to the research questions and relevant literature. Alternative methods, such as discourse and narrative analysis, were considered but rejected as the study aimed to explore broader organizational readiness rather than linguistic or narrative structures (Yin, 2014; Denscombe, 2010).

3.1 Method Application

This study employed a mixed-methods approach, integrating document review, questionnaires, and a semi-structured interview to collect and analyze data. The document review sourced diverse materials, including legal frameworks, industry standards, and EU legislation, to examine the potential influence of the new NIS2 Directive on the automotive sector. Articles and reports were selected based on their relevance to the research objectives, facilitating a comprehensive understanding of measures and practices applicable to the Directive's implementation. This foundational review informed the design of the questionnaire and interview guide. The questionnaire, pre-tested by cybersecurity professionals, was distributed electronically via platforms like LinkedIn and comprised both open-ended and closed-ended questions. It provided insights into industry readiness and trends. A semi-structured interview with the Chief Information Security Officer (CISO) of a leading European automotive company offered a deeper exploration of the company's cybersecurity practices and NIS2 compliance readiness. Conducted in Sweden, the interview focused on organizational security posture rather than auditing, with data transcribed and analyzed thematically. While additional interviews were planned, time constraints limited participation to one company.

This combined methodology strengthened the study by integrating diverse data sources, capturing both general trends and nuanced perceptions. Questionnaire findings highlighted organizational readiness trends, which were compared with qualitative insights from the interview. By blending qualitative and quantitative methods, the research offered a multidimensional view of the implications of the NIS2 Directive, focusing on patterns and preparedness rather than hypothesis testing, thus enhancing its ability to address the research question comprehensively.

4 RESULT

This result highlights the diverse implications that the new EU Directive will have on automotive industries within Sweden. Nineteen implications were discovered through thematic analysis of data obtained during the interview with a case study company. These implications were further categorised into Governance, Cybersecurity, Compliance and Regulatory Implications. Some of these implications were comparable to themes already discussed in earlier research on the impact of regulations and standards on various entities. However, this study identified implications that are delimited to the automotive sector while harping on extant frameworks, regulations, and standards relevant to Sweden's industry practices.

Respondents were asked about automotive companies' understanding of NIS2 obligations, with over 50% indicating moderate to high understanding. However, equal numbers highlighted either high or very low understanding levels. Challenges in determining NIS2 scope were acknowledged by seven respondents, with 50% identifying many challenges, 37.5% noting moderate challenges, and one respondent citing no challenge. Key obstacles included lack of clarity on enforcement, third-party compliance, supply chain security, and difficulties in recruiting cybersecurity talent.

Most respondents (75%) believe NIS2 is relevant to the automotive industry, though only 12.5% found communication from industry associations effective. Regarding readiness to meet NIS2 risk management requirements, none considered companies "Very Prepared," with 37.5% indicating "Partially Prepared," 25% "Not Prepared," and 12.5% "Well Prepared." Common obstacles included budget constraints, legacy system security, supply chain vulnerabilities, and limited expertise.

Respondents suggested industry best practices such as ISO 21434, ISO 27001, gap analyses, stakeholder education, and proper risk management to prepare for NIS2 compliance, with 50% finding these practices effective. To overcome challenges, professionals recommended tailored training, skilled workforce development, increased budgets, centralized resources, state-sponsored audits, and access to case studies on successful NIS2 readiness.

4.1 Governance Implications

Governance Implications. Organizational compliance efforts begin with management awareness of regulatory requirements, ensuring decision-making aligns with legal obligations. The case study company

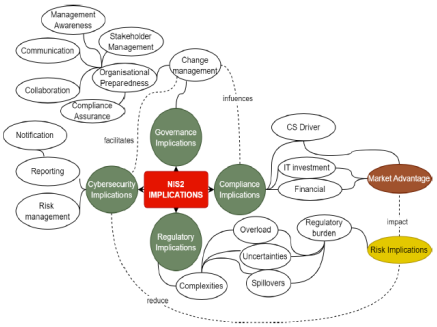

Figure 1: Thematic Map of identified themes and subthemes in an automotive company in Sweden.

demonstrated this awareness, with regulatory changes being communicated at the board level to guide compliance and avoid financial risks. Preparations for NIS2 compliance involve organizational changes, documentation, and collaboration among departments such as legal, IT, and R&D. Stakeholder communication and collaboration, including dialogues with competitors and regulatory bodies, are critical for addressing ambiguities in incident reporting and ensuring cohesive compliance strategies. Certifications, audits, and supply chain security mechanisms, such as TISAX, also play a vital role in the company's compliance assurance efforts.

Cybersecurity Implications. The study highlighted challenges with NIS2's updated reporting requirements, particularly in defining and addressing incidents and close calls. The company emphasized the need for robust Business Continuity and Disaster Recovery (BCP/BCM) processes to minimize the impact of cyberattacks. While NIS2 outlines basic requirements, supplementary frameworks like DORA provide greater specificity, including testing and documentation of BCP measures. Managing third-party security through certifications like TISAX further ensures supply chain integrity, with the company requiring suppliers to meet these standards for continued partnerships.

Regulatory and Compliance Implications. Regulatory complexity, including overlapping frameworks like GDPR and DORA, poses challenges for organizations operating across multiple countries. Variations in national implementations and reporting requirements create uncertainties, but NIS2 is seen as part of an ongoing regulatory journey. Compliance with such directives necessitates significant financial and IT investments, such as immutable storage systems, and drives organizational focus on cybersecurity beyond regulatory minimums. For premium brands, enhanced security is a competitive advantage, as modern consumers expect state-of-the-art cyber-

security to complement vehicle quality and performance, further underscoring the business imperative for robust cybersecurity measures.

5 DISCUSSION

Implications of NIS2 on the Automotive Sector. This study highlights the critical implications of the NIS2 Directive for the automotive sector, emphasizing the growing importance of cybersecurity as vehicles become increasingly connected and vulnerable to security threats. The study identified four key areas of impact: governance, compliance, cybersecurity, and regulatory challenges. Supply chain and third-party security emerged as a significant challenge, with 70% of respondents noting the complexities of ensuring NIS2 compliance among Original Equipment Manufacturers (OEMs) and their suppliers. Companies are adopting frameworks to monitor third-party involvement and secure components, reflecting efforts to align with NIS2 requirements.

The respondents expressed varying levels of understanding of NIS2 obligations, with most indicating moderate awareness, while some acknowledged gaps in clarity regarding specific provisions. Challenges cited include managing legacy systems, defining confidential information, and ensuring third-party compliance, compounded by resource constraints and limited expertise. These complexities align with broader regulatory risks and uncertainties noted in prior studies, highlighting the disruptive nature of new cybersecurity requirements that necessitate significant changes to processes, systems, and practices.

Despite these challenges, the study underscores the positive long-term impact of NIS2 in strengthening the automotive sector's cybersecurity posture. Automotive companies recognize the need to integrate security into the design phase of new technologies, leveraging international standards and frameworks to streamline compliance. While the regulatory burden may increase costs and complexity, respondents remain confident that NIS2 will drive resilience, enhance consumer trust, and provide a competitive edge for brands prioritizing robust cybersecurity measures. Investments in training, automation, and scalable solutions are crucial for adapting to this evolving regulatory landscape and ensuring a secure automotive ecosystem.

5.1 Novelty

According to Kianpour and Raza (2024), an adaptable compliance framework can optimise resources

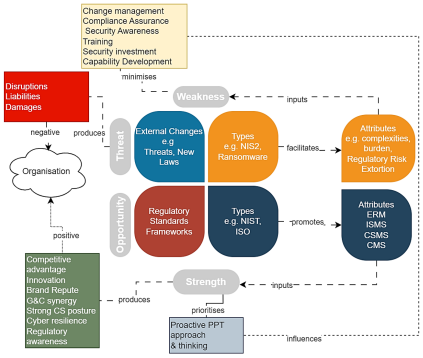

Figure 2: Opportunity Exchange Matrix.

and ensure a consistent approach to compliance when integrated with other organisational practices. Building on this, the study developed an Opportunity Exchange Matrix (see Figure 8) as a tool to visualize the relationships between internal and external factors influencing an organisation. While not a formal framework, the matrix serves as a compliance tool, helping organisations map cybersecurity threats and identify corresponding opportunities to enhance resilience. The Opportunity Exchange Matrix adopts concepts from SWOT analysis to categorize and compare cybersecurity threats and opportunities within the automotive sector. It enables organisations to transform identified threats into strengths by leveraging different types of cybersecurity opportunities. This adaptable approach, already observed in the automotive industry, is further encouraged by the matrix.

In this model, external changes can act as both threats and opportunities, impacting organisations either positively or negatively. The matrix visualizes how cybersecurity opportunities can counter these threats, building organisational strength while minimizing weaknesses. By outlining key attributes of cybersecurity threats, the matrix highlights how organisations can align compliance requirements with using the controls from cybersecurity opportunities to streamline best practices. Additionally, the matrix helps analyse how internal strengths are built and how organisational weaknesses are mitigated through the effective use of cybersecurity opportunities.

The figure below presents an alignment of relevant frameworks, standards, and guidelines that can be utilised for automotive cybersecurity.

This study reveals how the NIS2 Directive is perceived within the automotive industry, especially in terms of the external complexities it introduces. Regulatory changes like NIS2 often create uncertainties and challenges, particularly for sectors such as automotive, which are considered heavily regulated

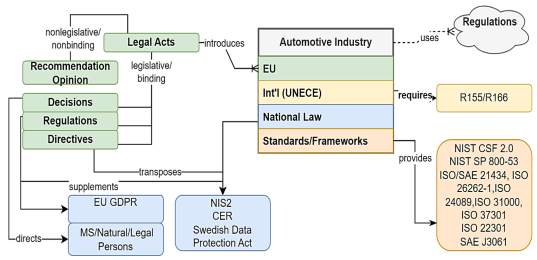

Figure 3: Alignment of some relevant regulatory frameworks for automotive cybersecurity.

(Kalogeraki & Polemi, 2024). These external influencers, often perceived as regulatory overload, produce regulatory burdens that can generate organisational weaknesses if not managed effectively. However, the study shows that an organisation's internal responses to these external influences play a critical role in determining whether such changes result in weaknesses or strengths.

For the automotive sector, understanding how to navigate these complexities is crucial. The findings of this study highlight that external influencers, such as new regulations, can also present opportunities. When leveraged correctly, these opportunities can help reinforce internal strengths and improve organisational resilience. The Opportunity Exchange Matrix developed in this study provides a practical tool for organisations to assess their readiness for regulatory changes and emerging threats. By mapping how external challenges can be converted into organisational strength, the matrix helps organisations evaluate their position in a proactive, structured manner.

The matrix provides a quick assessment of an organisation's readiness to respond to external threats, such as regulatory changes or AI advancements. These disruptions will continue to have significant implications for the automotive sector. By using the matrix, organisations can analyse how cybersecurity opportunities (such as in Figure 9) can be converted into strengths, which in turn minimize, mitigate, or capitalize on the impact of cybersecurity threats when addressed proactively.

5.2 Implications for Practice and Theory

The study's findings have several implications for theory in the field of cybersecurity and regulatory compliance. Firstly, it reinforces the idea that government mandates, like NIS2, can act as catalysts for improving cybersecurity practices across industries. The study supports the theoretical perspective that compliance frameworks drive organisational behaviour and resource allocation toward more secure operational

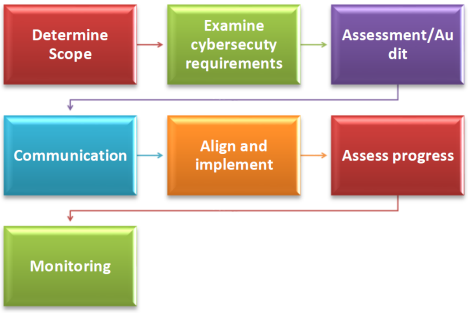

Figure 4: NIS2 Compliance Checklist.

environments (Hasan et al., 2021). From this standpoint, the study supports the idea that government regulations, such as NIS2, are key drivers of organisational change in cybersecurity. It reinforces that compliance frameworks influence companies to invest in stronger cybersecurity measures, aligning with theoretical views on regulatory-driven behaviour (Hasan et al., 2021).

The study's findings have several implications for theory in the field of cybersecurity and regulatory compliance. Firstly, it reinforces the idea that government mandates, like NIS2, can act as catalysts for improving cybersecurity practices across industries. The study supports the theoretical perspective that compliance frameworks drive organisational behaviour and resource allocation toward more secure operational environments (Hasan et al., 2021). From this standpoint, the study supports the idea that government regulations, such as NIS2, are key drivers of organisational change in cybersecurity. It reinforces that compliance frameworks influence companies to invest in stronger cybersecurity measures, aligning with theoretical views on regulatory-driven behaviour (Hasan et al., 2021).

6 CONCLUSION

This research explores the anticipated impacts of the NIS2 Directive on cybersecurity practices and compliance within the Swedish automotive industry. The study identifies key regulatory, governance, cybersecurity, and compliance implications, highlighting challenges, preparedness levels, and future outlooks. As vehicles become increasingly connected, the industry faces heightened cybersecurity risks, and NIS2 introduces new measures that impose significant changes to existing practices, creating regulatory complexity and financial burdens. However, the integration of existing standards and best practices provides a foundation for navigating these challenges and

aligning with legislative intentions. The study emphasizes the importance of organizational preparedness and the strategic use of supplemental industry standards to enhance compliance agility. Leveraging these practices helps moderate regulatory burdens while improving resilience and proactiveness. Despite gaps in awareness and readiness among automotive companies, cybersecurity readiness can optimize compliance efforts and improve security performance. Effective change management and multi-stakeholder collaboration are crucial for achieving the goals of NIS2 and maintaining operational agility amidst evolving regulatory and threat landscapes.

Finally, cybersecurity is not only critical for compliance but also a key driver of brand value and market influence in the automotive sector. By exceeding regulatory requirements and embedding security into design and operational strategies, companies can enhance consumer trust and competitive advantage. The study underscores the necessity of continuous adaptation to regulatory changes, emphasizing that preparedness, strategic investment, and resilience are pivotal for long-term success in an increasingly complex cybersecurity environment. Future research could explore several areas beyond the scope of this study. Investigating security as a differentiator for premium automotive brands could validate how customer perceptions of cybersecurity influence brand differentiation and purchasing decisions. Comparative studies of NIS2 implementation across European countries could identify best practices and ethical considerations in balancing transparency with national security. Additionally, examining cybersecurity awareness and training programs within the Swedish automotive sector could reveal knowledge gaps and improvements to enhance workforce readiness. Exploring future regulatory scenarios and industry collaboration could provide insights into navigating cybersecurity challenges and opportunities, informing policy development and fostering a secure digital ecosystem in Sweden and the EU.

REFERENCES

Babikian, J. (2023). Navigating Legal Frontiers: Exploring Emerging Issues in Cyber Law. *Revista Espanola de Documentacion Cientifica*, 17(2), 95–109. https://doi.org/10.13140/RG.2.2.20264.55048

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

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

BreachRx. (2020, March 25). Emerging Regulations Increase Complexity for Risk Management. A BreachRx.

Costantino, G., De Vincenzi, M., & Matteucci, I. (2022). In-Depth Exploration of ISO/SAE 21434 and Its Correlations with Existing Standards. *IEEE Communications Standards Magazine*, 6(1), 84–92. https://doi.org/10.1109/MCOMSTD.0001.2100080

Denscombe, M. (2010a). The Good Research Guide: For Small-scale Social Research Projects.

Denscombe, M. (2010b). The Good Research Guide: For Small-scale Social Research Projects (4th ed.). *Open University Press*.

Denscombe, M. (2014). The Good Research Guide: For Small-Scale Social Research Projects (5th ed.). *McGraw-Hill/Open University Press*.

Edgar, T. W., & Manz, D. O. (2017). Chapter 5 - Descriptive Study. In T. W. Edgar & D. O. Manz (Eds.), Research Methods for Cyber Security (pp. 3–31). Syngress. https://doi.org/10.1016/B978-0-12-805349-2.00001-7

EU Cybersecurity Index. (2024). www.enisa.europa.eu.

European Commission. (2020). Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

Fumy, W. (2004). IT security standardisation. Network Security, 2004(12), 6–11.

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2017). Resilience of cyber systems with over-and underregulation. Risk Analysis, 37(9), 1644–1651.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., Zhou, L., & others. (2014). Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model. *Journal of Information Security*, 6(01), 24.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 19(1), 33–56.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58, 102726.

Hill, M. (2023, September 14). Automotive supply chain vulnerable to attack as cybersecurity regulation looms. An IDG, Inc, Company.

Hiscox Report. (2023). Hiscox Cyber Readiness Report. https://www.hiscoxgroup.com/cyber-readiness

Hoffmann, V. H., Trautmann, T., & Hamprecht, J. (2009). Regulatory uncertainty: A reason to postpone investments? Not necessarily. *Journal of Management Studies*, 46(7), 1227–1253.

Jeong, C. Y., Lee, S.-Y. T., & Lim, J.-H. (2019). Information security breaches and IT security investments: Impacts on competitors. In-

formation & Management, 56(5), 681–695. https://doi.org/10.1016/j.im.2018.11.003

Johannesson, P., & Perjons Erik. (2014). An Introduction to Design Science. *Springer International Publishing*.

Kalogeraki, E.-M., & Polemi, N. (2024). A taxonomy for cybersecurity standards. *Journal of Surveillance, Security and Safety*, 5(2), 95–115. https://doi.org/10.20517/jsss.2023.50

Babikian, J. (2023). Navigating Legal Frontiers: Exploring Emerging Issues in Cyber Law. *Revista Espanola de Documentacion Cientifica, 17*(2), 95–109. https://doi.org/10.13140/RG.2.2.20264.55048

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

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

BreachRx. (2020, March 25). Emerging Regulations Increase Complexity for Risk Management. *A BreachRx.*

Costantino, G., De Vincenzi, M., & Matteucci, I. (2022). In-Depth Exploration of ISO/SAE 21434 and Its Correlations with Existing Standards. *IEEE Communications Standards Magazine, 6*(1), 84–92. https://doi.org/10.1109/MCOMSTD.0001.2100080

Denscombe, M. (2010a). *The Good Research Guide: For Small-scale Social Research Projects.*

Denscombe, M. (2010b). *The Good Research Guide: For Small-scale Social Research Projects* (4th ed.). Open University Press.

Denscombe, M. (2014). *The Good Research Guide: For Small-Scale Social Research Projects* (5th ed.). McGraw-Hill/Open University Press.

Edgar, T. W., & Manz, D. O. (2017). Chapter 5 - Descriptive Study. In T. W. Edgar & D. O. Manz (Eds.), *Research Methods for Cyber Security* (pp. 3–31). Syngress. https://doi.org/10.1016/B978-0-12-805349-2.00001-7

EU Cybersecurity Index. (2024). *www.enisa.europa.eu.*

European Commission. (2020). Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

Fumy, W. (2004). IT security standardisation. *Network Security, 2004*(12), 6–11.

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2017). Resilience of cyber systems with over-and underregulation. *Risk Analysis, 37*(9), 1644–1651.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., Zhou, L., & others. (2014). Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model. *Journal of Information Security, 6*(01), 24.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19*(1), 33–56.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications, 58,* 102726.

Hill, M. (2023, September 14). Automotive supply chain vulnerable to attack as cybersecurity regulation looms. *An IDG, Inc, Company.*

Hiscox Report. (2023). *Hiscox Cyber Readiness Report*. https://www.hiscoxgroup.com/cyber-readiness

Hoffmann, V. H., Trautmann, T., & Hamprecht, J. (2009). Regulatory uncertainty: A reason to postpone investments? Not necessarily. *Journal of Management Studies, 46*(7), 1227–1253.

Jeong, C. Y., Lee, S.-Y. T., & Lim, J.-H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management, 56*(5), 681–695. https://doi.org/10.1016/j.im.2018.11.003

Johannesson, P., & Perjons Erik. (2014). An Introduction to Design Science. *Springer International Publishing.*

Kalogeraki, E.-M., & Polemi, N. (2024). A taxonomy for cybersecurity standards. *Journal of Surveillance, Security and Safety, 5*(2), 95–115. https://doi.org/10.20517/jsss.2023.50

Babikian, J. (2023). Navigating Legal Frontiers: Exploring Emerging Issues in Cyber Law. *Revista Espanola de Documentacion Cientifica, 17*(2), 95–109. https://doi.org/10.13140/RG.2.2.20264.55048

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

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

BreachRx. (2020, March 25). Emerging Regulations Increase Complexity for Risk Management. *A BreachRx.*

Costantino, G., De Vincenzi, M., & Matteucci, I. (2022). In-Depth Exploration of ISO/SAE 21434 and Its Correlations with Existing Standards. *IEEE Communications Standards Magazine, 6*(1), 84–92. https://doi.org/10.1109/MCOMSTD.0001.2100080

Denscombe, M. (2010a). The Good Research Guide: For Small-scale Social Research Projects.

Denscombe, M. (2010b). The Good Research Guide: For Small-scale Social Research Projects (4th ed.). *Open University Press.*

Denscombe, M. (2014). The Good Research Guide: For Small-Scale Social Research Projects (5th ed.). *McGraw-Hill/Open University Press.*

Edgar, T. W., & Manz, D. O. (2017). Chapter 5 - Descriptive Study. In T. W. Edgar & D. O. Manz (Eds.), Research Methods for Cyber Security (pp. 3–31). *Syngress.* https://doi.org/10.1016/B978-0-12-805349-2.00001-7

EU Cybersecurity Index. (2024). *www.enisa.europa.eu.*

European Commission. (2020). Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

Fumy, W. (2004). IT security standardisation. *Network Security, 2004*(12), 6–11.

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2017). Resilience of cyber systems with over-and underregulation. *Risk Analysis, 37*(9), 1644–1651.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., Zhou, L., & others. (2014). Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model. *Journal of Information Security, 6*(01), 24.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? Journal of Computer Security, 19(1), 33–56.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. Journal of Information Security and Applications, 58, 102726.

Hill, M. (2023, September 14). Automotive supply chain vulnerable to attack as cybersecurity regulation looms. *An IDG, Inc, Company.*

Hiscox Report. (2023). Hiscox Cyber Readiness Report. https://www.hiscoxgroup.com/cyber-readiness

Hoffmann, V. H., Trautmann, T., & Hamprecht, J. (2009). Regulatory uncertainty: A reason to postpone investments? Not necessarily. *Journal of Management Studies, 46*(7), 1227–1253.

Jeong, C. Y., Lee, S.-Y. T., & Lim, J.-H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management, 56*(5), 681–695. https://doi.org/10.1016/j.im.2018.11.003

Johannesson, P., & Perjons Erik. (2014). An Introduction to Design Science. *Springer International Publishing.*

Kalogeraki, E.-M., & Polemi, N. (2024). A taxonomy for cybersecurity standards. *Journal of Surveillance, Security and Safety, 5*(2), 95–115. https://doi.org/10.20517/jsss.2023.50