Journal of Next-Generation Research 5.0 (JNGR 5.0)
ISSN: **3075-2868** Website: www.jngr5.com Email: editor@jngr5.com

Empirical Analysis of NIS2 Adoption in EU SMEs: Challenges for Critical Infrastructure in Germany

Thomas Joswig[1], Walter Kurz[1]

[1]Signum Magnum College, Malta
Contributing authors: thomas.joswig@smc.college; walter.kurz@smc.college;

Abstract

This research investigates the implementation of the NIS2 Directive in small and medium-sized enterprises (SMEs) categorised as part of critical infrastructure in Germany. The study examines regulatory requirements, compliance challenges, and the practical implications of cybersecurity obligations under NIS2, with particular emphasis on SMEs' resource limitations and sector-specific vulnerabilities. A mixed-method approach was utilised, integrating qualitative analysis of legal frameworks, academic literature, and policy guidelines with quantitative survey data from SMEs operating in critical sectors. This methodological design facilitates a comprehensive assessment of both regulatory demands and real-world compliance barriers. The findings indicate that SMEs encounter substantial challenges in interpreting and implementing NIS2 requirements, with compliance scores exhibiting variation across company size and industry sector. While larger SMEs in telecommunications and energy demonstrate moderate preparedness (mean score 72.3), smaller enterprises in service-based sectors manifest lower compliance levels (mean score 48.5). Principal obstacles comprise financial constraints, limited cybersecurity expertise, and the complexity of mandatory risk management and reporting obligations. The study elucidates the disproportionate burden that NIS2 imposes on SMEs in comparison to larger enterprises. The absence of tailored cybersecurity frameworks and financial support mechanisms exacerbates compliance challenges, particularly in resource-limited sectors. Incident reporting obligations and supply chain security requirements introduce additional administrative and operational encumbrances, necessitating sector-specific guidance and targeted assistance. Ensuring SME compliance with NIS2 necessitates regulatory modifications, financial incentives, and pragmatic support measures. Policy recommendations encompass simplified compliance frameworks, government-supported cybersecurity advisory services, and enhanced funding for SME cybersecurity initiatives. The development of sector-specific guidelines, AI-driven compliance tools, and targeted training programmes could reduce administrative burdens while enhancing cybersecurity resilience. A risk-based approach, aligned with SMEs' operational realities, is imperative to balance cybersecurity resilience

with economic viability.

Keywords: NIS2, SMEs, Cybersecurity Compliance, Critical Infrastructure, Regulatory Challenges, Risk Management, Incident Reporting, AI-Driven Compliance

1 Introduction

The Network and Information Security Directive 2 (NIS2) is the European Union's updated regulatory framework aimed at strengthening cybersecurity across critical infrastructure sectors [1]. Replacing the original NIS Directive, NIS2 introduces stricter security requirements and extends its scope to a wider range of organisations, including small and medium-sized enterprises (SMEs) that provide essential services. While these measures seek to enhance cybersecurity resilience, compliance poses significant challenges for SMEs due to financial, technical, and organisational constraints.

Germany's critical infrastructure (KRITIS) sectors—including energy, healthcare, finance, and digital services—are now subject to enhanced risk management and incident reporting mandates under NIS2 [2]. SMEs operating in these industries face considerable barriers to compliance, particularly due to limited resources and expertise. Empirical findings suggest that while larger SMEs in telecommunications and energy report moderate levels of compliance readiness (mean score 72.3), smaller enterprises in service-based sectors exhibit significantly lower preparedness (mean score 48.5) [3]. Key challenges include high compliance costs, a lack of cybersecurity personnel, and ambiguities in interpreting risk assessment and supply chain security requirements [4].

Research on cybersecurity has focused largely on technical risk mitigation, while the economic impact on SMEs remains underexplored [5]. This study applies economic theory to cybersecurity by framing it within market failure and the concept of socially beneficial services [6, 7]. Cybersecurity generates positive externalities that extend beyond the individual firm, contributing to broader societal security [18, 31]. SMEs often underinvest in cybersecurity due to information asymmetry and financial constraints. Addressing this gap may require regulatory measures and governmental intervention [6, 8].

External pressures also drive cybersecurity adoption. The global cybersecurity landscape has changed due to rising data privacy concerns. Investor confidence is increasingly linked to regulatory compliance, particularly in data-intensive sectors such as healthcare and connected vehicle applications [9, 10]. The adoption of Industry 4.0 technologies has expanded cybersecurity risks, as ICT and IT systems become integral to business operations [11]. Regulatory frameworks such as the General Data Protection Regulation (GDPR) in Europe require stricter privacy and security measures [12, 13, 14]. NIS2 compliance must be considered alongside these broader regulatory obligations.

This study analyses the compliance challenges SMEs face in Germany's KRITIS sectors under NIS2. A mixed-method approach integrates qualitative legal analysis with empirical survey data to assess sector- specific disparities. The research contributes to policy discussions on regulatory efficiency and the need for targeted support

mechanisms that balance cybersecurity resilience with economic feasibility.

1.1 Related work and research gaps

The implementation of the NIS2 Directive presents significant challenges for small and medium-sized enterprises (SMEs) in Germany's critical infrastructure sectors. Grant Thornton [15] highlight that the directive introduces stricter security requirements, necessitating substantial technical and organizational changes, which may disproportionately affect German SMEs due to their limited resources. The expanded scope of NIS2 encompasses additional sectors, including postal and courier services, waste management, and chemical industries, thereby increasing the compliance burden on SMEs operating within these domains [16]. The directive also imposes comprehensive risk management measures and stringent reporting obligations, requiring SMEs to allocate significant resources towards compliance efforts [17]. As of January 2025, Germany has not yet transposed the NIS2 Directive into national law, resulting in legal uncertainties for affected companies [17]. This delay exacerbates the challenges faced by SMEs, as they must navigate compliance requirements amidst evolving regulatory landscapes. Collectively, these studies underscore the pressing need for tailored support mechanisms and clear regulatory guidance to assist SMEs in achieving compliance with the NIS2 Directive. Despite the increasing importance of cybersecurity in the digital economy, significant research gaps remain regarding the effective implementation of security measures in SMEs.

Existing cybersecurity literature primarily focuses on risk assessment frameworks, technical solutions, and regulatory compliance, with little attention to the practical challenges faced by different stakeholders in SMEs. Research highlights that cybersecurity decision-making varies significantly among business owners, IT personnel, and third-party security providers, each of whom has different priorities and levels of awareness. This discrepancy leads to inconsistent cybersecurity adoption and gaps in implementation, particularly in SMEs with limited in-house expertise [18, 19]. Future research should employ multi-stakeholder qualitative approaches to explore these diverse perspectives and develop more inclusive cybersecurity policies.

Cybersecurity adoption in SMEs is shaped by a combination of internal motivations and external pressures. Ethical responsibility, consumer trust, and perceived vulnerability influence SMEs' willingness to invest in cybersecurity measures [20]. At the same time, SMEs must comply with regulatory frameworks such as GDPR in Europe while also responding to evolving cyber threats and industry expectations. Current research does not fully address how SMEs balance these competing influences or the financial and operational constraints that impact their cybersecurity investments [21]. Future studies should examine which regulatory and financial strategies best enable SMEs to implement cybersecurity measures without disproportionate cost burdens.

While cybersecurity frameworks such as ISO/IEC 27001 and NIST guidelines provide well-established best practices, they are often too complex, resource-intensive, and costly for SMEs. Unlike large enterprises, SMEs lack dedicated cybersecurity teams, making compliance with these standards challenging [22]. No widely adopted cybersecurity framework is specifically designed for SMEs, leaving many businesses

without clear guidance on practical, scalable cybersecurity implementation [23]. Future research should focus on developing simplified, SME-friendly cybersecurity standards and exploring government incentives, regulatory adjustments, and financial support mechanisms to encourage adoption without imposing excessive administrative burdens.

Another key issue is the lack of cybersecurity awareness and training among SME employees. Many cybersecurity breaches stem from human error, highlighting the need for training programs that go beyond theoretical knowledge to focus on practical behavioral changes that reduce security risks. Policymakers should introduce incentives such as subsidies or certification programs to encourage SMEs to actively invest in cybersecurity education.

A major concern is that SMEs often take a reactive rather than proactive approach to cybersecurity, implementing security measures only after experiencing an attack. To mitigate this risk, governments and industry organizations should provide financial incentives, such as tax reductions, grants, or subsidies, to encourage SMEs to invest proactively in cybersecurity infrastructure.

Many SMEs also lack direct access to cybersecurity experts and industry knowledge, which hinders their ability to implement effective security strategies. Strengthening collaboration between SMEs, cybersecurity professionals, and industry organizations would ensure that SMEs stay updated on best practices and emerging threats. Public-private partnerships could play a key role in helping SMEs gain access to affordable cybersecurity services and expertise.

There is a noticeable gap in empirical research on cybersecurity risk management in SMEs, particularly in developing economies, where awareness and regulatory enforcement remain limited. Future studies should explore the longitudinal effects of cybersecurity strategies in SMEs to identify the most effective and sustainable solutions for long-term protection against cyber threats.

SMEs require tailored cybersecurity policies, enhanced awareness programs, financial support mechanisms, and stronger collaboration with cybersecurity experts to develop a more resilient cybersecurity posture. Addressing these gaps will not only protect SMEs from evolving cyber threats but also contribute to strengthening overall digital security ecosystems on both national and global scales [24].

Despite the growing regulatory focus on cybersecurity, research on SME compliance remains fragmented. Existing studies address regulatory requirements but often fail to provide actionable insights into how SMEs can overcome structural constraints to meet these obligations. The literature lacks empirical evaluations of sector-specific cybersecurity adoption and the financial impact of compliance measures, particularly for SMEs in critical infrastructure sectors. There is insufficient research on how SMEs perceive regulatory complexity and whether existing cybersecurity standards align with their operational needs.

The lack of longitudinal studies also limits understanding of how cybersecurity strategies evolve over time within SMEs. Future research should assess the effectiveness of different policy interventions, financial incentives, and industry-specific regulatory adaptations. Cross-country comparative analyses are needed to examine how

variations in national implementation of directives such as NIS2 influence SME cybersecurity outcomes.

1.2 Contribution of this research

Existing research on SME cybersecurity compliance has primarily focused on general risk management frameworks and the challenges of large enterprises. While studies highlight that SMEs are highly vulnerable to cyber threats [25], fewer works examine the sector-specific compliance difficulties SMEs face under NIS2. Research indicates that many SMEs lack the necessary expertise and financial resources to meet regulatory requirements, leading to inconsistent implementation across industries [5, 26]. Although prior work has discussed cybersecurity governance for SMEs [5], there remains a gap in empirical research addressing the implications of NIS2 compliance within KRITIS sectors.

This study contributes to the literature by providing an empirical analysis of SME compliance with NIS2, with a focus on sector-specific disparities and regulatory challenges. Unlike existing research, which predominantly discusses theoretical cybersecurity frameworks, this study integrates quantitative survey data to measure actual compliance levels across industries. By identifying practical obstacles and policy gaps, the research offers actionable recommendations for regulatory bodies and industry stakeholders to develop tailored compliance support mechanisms for SMEs.

The findings inform policymakers on how to refine cybersecurity regulations to balance regulatory enforcement with economic feasibility, ensuring that SMEs can comply with NIS2 without excessive financial burden.

2 The NIS directive and the evolution to NIS2

The Network and Information Security (NIS) Directive, officially known as Directive (EU) 2016/1148, was the European Union's first legislative framework designed to enhance cybersecurity resilience across Member States. Implemented in August 2016, the directive established a regulatory foundation for securing network and information systems, particularly for entities operating in sectors critical to the economy and society. It required each Member State to adopt a national cybersecurity framework, introduce security requirements for designated operators of essential services (OES) and digital service providers (DSPs), and establish mechanisms for cross-border cooperation in handling cybersecurity incidents [27].

The directive mandated that Member States develop comprehensive national cybersecurity strategies, including governance structures for risk management, preparedness measures for cyber incidents, and mechanisms for responding to cybersecurity threats. Each Member State was required to designate national competent authorities responsible for enforcing the directive and ensuring compliance. Computer Security Incident Response Teams (CSIRTs) were introduced to improve cybersecurity coordination at the national and EU levels. These teams were tasked with monitoring cybersecurity incidents, issuing alerts and early warnings, conducting risk analyses, and increasing situational awareness. Organizations subject to the directive were obligated to implement cybersecurity risk management measures and report significant security

incidents to relevant national authorities [28].

Despite these regulatory advancements, the implementation of the original NIS Directive faced significant challenges. One of the primary issues was the flexibility granted to Member States in transposing the directive into national law, leading to discrepancies in enforcement and compliance measures. Some countries adopted stricter cybersecurity requirements, while others took a more lenient approach, resulting in a fragmented cybersecurity landscape across the EU. Digital service providers faced fewer regulatory obligations compared to operators of essential services, despite playing a crucial role in the digital economy. Another notable challenge was the lack of coordination between the NIS Directive and the General Data Protection Regulation (GDPR), as both regulations imposed security and reporting obligations that sometimes overlapped or conflicted with each other. The rapidly evolving cyber threat landscape also exposed limitations in the directive's framework, particularly regarding supply chain vulnerabilities, AI-driven cyberattacks, and the increasing frequency of ransomware incidents [1].

In response to these challenges, the European Union introduced the NIS2 Directive (Directive (EU) 2022/2555), which came into force on January 16, 2023, and will be applicable from October 18, 2024. The updated directive aims to address the shortcomings of its predecessor by expanding its scope, strengthening enforcement mechanisms, and introducing more stringent security requirements. One of the key changes in NIS2 is the extension of its applicability to a broader range of sectors and organizations. Unlike the original directive, which categorized entities as operators of essential services and digital service providers, NIS2 introduces two new classifications: Essential Entities (EE) and Important Entities (IE). Essential Entities include large organizations in critical sectors such as energy, banking, healthcare, transport, and digital infrastructure. Important Entities include medium-sized businesses operating in sectors such as waste management, postal services, and manufacturing. This reclassification ensures that more businesses fall under the directive's requirements, thereby strengthening the overall cybersecurity resilience of the EU [29].

2.1 Regulatory framework and compliance obligations

NIS2 also introduces stricter cybersecurity measures that all covered organizations must implement. These measures include risk management frameworks, incident prevention, detection, and response mechanisms, supply chain security assessments, and encryption standards for data protection. Organizations are required to conduct regular cybersecurity audits and implement employee awareness and training programs to mitigate risks associated with human error. The directive imposes more stringent reporting obligations for cybersecurity incidents. Entities must report significant cyber incidents to their national cybersecurity authority within 24 hours of detection, submit a follow-up report within 72 hours, and provide a comprehensive impact assessment within one month. Failure to report incidents in a timely manner can result in severe financial penalties, highlighting the EU's commitment to enhancing cybersecurity transparency and accountability [30].

2.2 Impact of NIS2 on critical infrastructure and SMEs

The enforcement and supervision of cybersecurity measures have also been strengthened under NIS2. National competent authorities are granted enhanced supervisory powers, including the ability to conduct on-site and remote audits, request access to cybersecurity policies, and issue corrective action orders in cases of non-compliance. The directive introduces harmonized penalties for non-compliance, with Essential Entities facing fines of up to €10 million or 2% of their global annual revenue, while Important Entities may be fined up to €7 million or 1.4% of their global annual revenue. Company executives can be held personally accountable for failing to implement adequate cybersecurity measures, further emphasizing the importance of compliance [29].

Another major component of NIS2 is its focus on supply chain security and third-party risk management. Organizations are required to assess and mitigate cybersecurity risks across their entire supply chain, including third-party service providers. This requirement aims to address vulnerabilities arising from outsourced IT services, cloud computing dependencies, and software supply chain threats. NIS2 seeks to improve cooperation between EU Member States by establishing a unified cyber crisis response framework known as *EU CyCLONe* (Cyber Crisis Liaison Organization Network). This initiative is designed to facilitate coordinated responses to large-scale cyber incidents, enabling faster information sharing and collective decision-making among Member States [28].

While NIS2 represents a significant step forward in strengthening cybersecurity across the EU, it also introduces new challenges, particularly for small and medium-sized enterprises (SMEs). Many SMEs that were not previously subject to NIS regulations are now required to comply with the updated directive, increasing their cybersecurity responsibilities. A major challenge for SMEs is the financial and human resource burden associated with implementing comprehensive security measures. Unlike large corporations with dedicated cybersecurity teams, SMEs often lack the expertise and budget to meet these new requirements. The need for investments in cybersecurity technologies, training programs, and compliance monitoring places additional strain on SMEs, potentially affecting their operational viability [31].

The complexity of NIS2 compliance poses difficulties for SMEs that lack structured cybersecurity strategies. Many SMEs struggle with implementing incident response plans, conducting risk assessments, and ensuring compliance with supply chain security obligations. The stringent incident reporting requirements, which mandate notification of cyber incidents within 24 hours, pose an additional challenge, as many SMEs do not have dedicated security personnel to handle real-time cyber threat monitoring and response. The potential financial penalties for non-compliance create a significant risk for SMEs, as failure to meet NIS2 requirements can result in substantial fines and reputational damage.

The transition from the original NIS Directive to NIS2 reflects the EU's commitment to enhancing cybersecurity resilience across its Member States. The expanded scope, stricter security measures, and strengthened enforcement mechanisms aim to address the shortcomings of its predecessor and create a more unified cybersecurity framework

across the EU. The directive also presents new challenges, particularly for SMEs, which require additional support mechanisms such as financial incentives, regulatory guidance, and tailored cybersecurity frameworks to achieve compliance without disproportionate cost burdens.

2.3 Key gaps in NIS2 implementation for SMEs

Despite the expanded scope and stricter requirements introduced by the NIS2 Directive, significant gaps remain in its implementation, particularly for small and medium-sized enterprises (SMEs). A major issue is the lack of awareness among SMEs regarding their obligations under the directive, leading to delays in compliance efforts and uncertainty in regulatory adaptation. Many SMEs operate with outdated or insufficient IT infrastructure, making it challenging to meet the enhanced security requirements mandated by NIS2. Additionally, the absence of standardized cybersecurity processes, such as formal risk assessment frameworks and structured incident response mechanisms, poses a significant compliance barrier.

The directive also presents specific challenges for data centers, which are subject to multiple regulatory frameworks, including the GDPR, NIS2, and industry standards such as EN 50600. Despite these comprehensive regulations, gaps persist, particularly concerning the security of modern AI-driven technologies. AI systems rely heavily on vast amounts of data and are increasingly vulnerable to AI-generated threats, such as adversarial attacks. While NIS2 strengthens security requirements for data centers, it does not provide explicit guidelines for safeguarding highly sensitive AI-related data, creating a regulatory blind spot. Current cybersecurity standards have yet to fully address the evolving threats associated with AI technologies, leaving critical infrastructure exposed to emerging risks [1].

3 Methodology

The study employs a mixed-method approach, integrating qualitative legal analysis with quantitative empirical data. It examines compliance challenges faced by Small and Medium-sized Enterprises (SMEs) in Germany's critical infrastructure sectors (KRITIS) under the NIS2 Directive.

3.1 Research approach

The research follows a mixed-method framework, combining legal analysis with empirical survey data to evaluate SME readiness for NIS2 compliance. The qualitative component examines cybersecurity obligations under NIS2, while the quantitative component gathers structured survey data on compliance challenges. Integrating these approaches provides both regulatory insights and practical evidence, addressing the gap between legal mandates and SME operational constraints.

3.2 Data collection

This study relies on two primary data sources: a legal black-letter analysis of NIS2 compliance requirements and an empirical survey of SMEs in Germany's critical infrastructure sectors. The legal analysis examines risk management requirements, incident reporting obligations, and sector-specific regulatory interpretations.

The review includes documents from the European Commission, the European Union

Agency for cybersecurity (ENISA), and Germany's Federal Office for Information Security (BSI). It evaluates how national implementation efforts shape compliance burdens and identifies ambiguities in enforcement. The empirical survey assesses SME cybersecurity readiness and challenges in implementing NIS2. It investigates security practices, awareness of regulatory obligations, and compliance barriers related to financial, technical, and personnel constraints. A stratified sampling method ensures broad representation across KRITIS sectors. The survey captures sector-specific compliance variations and highlights disparities in regulatory adaptation.

3.3 Survey design

The survey measures compliance readiness and implementation challenges among SMEs in Germany's critical infrastructure sectors. A structured design ensures reliable and representative data collection across industries subject to NIS2.

3.3.1 Sample selection

Stratified sampling ensures adequate representation of SMEs from all KRITIS sectors, including energy, healthcare, transportation, finance, and digital services. Eligibility requires businesses to meet the European Commission's SME definition and operate within NIS2-regulated industries. Participants were identified through industry associations, cybersecurity advisory bodies, and public business registries. A total of 27 expert respondents from specialised SMEs participated in the survey, ensuring sector-specific insights into compliance challenges. The selection process captures a diverse range of SMEs, accounting for differences in size, revenue, and cybersecurity maturity.

3.3.2 Industry segmentation

SMEs were categorized based on primary industry classification following the official KRITIS sector definitions outlined by Germany's Federal Office for Information Security (BSI). The segmentation accounts for variations in regulatory exposure, resource availability, and cybersecurity maturity.

3.3.3 Survey structure

The survey consists of quantitative and qualitative components. The quantitative section employs a five- point Likert scale to assess SME familiarity with NIS2 requirements, perceived compliance readiness, and resource availability for cybersecurity implementation. Respondents evaluate their ability to meet obligations related to risk management, incident reporting, and supply chain security. The qualitative section includes open-ended questions to identify specific compliance challenges. These questions explore financial constraints, cybersecurity expertise gaps, and regulatory uncertainty. Sections assess SME engagement with external cybersecurity advisory services and perspectives on government support mechanisms. The survey was distributed electronically through SME networks, industry forums, and cybersecurity organizations. Responses were collected over a defined period to ensure comprehensive data coverage across KRITIS sectors.

3.4 Data Analysis

The data collected from the survey and legal analysis was processed using quantitative and qualitative methods. Statistical analysis was applied to the survey responses to evaluate SME compliance readiness across KRITIS sectors, while qualitative coding

techniques were used to interpret open-ended responses regarding compliance challenges. This dual approach ensures a comprehensive assessment of NIS2 implementation among SMEs.

3.4.1 Quantitative Data Analysis

Survey responses were analyzed using descriptive and inferential statistical methods. Mean scores and standard deviations were calculated to assess SME familiarity with NIS2, compliance readiness, and the availability of financial and technical resources. Comparative analysis was conducted across KRITIS sectors to identify sector-specific disparities in compliance levels.

Correlation analysis was applied to explore relationships between SME size, industry type, and compliance readiness. Regression models were used to examine the impact of financial and technical constraints on compliance performance. Where applicable, clustering techniques were employed to group SMEs based on similarities in compliance challenges.

3.4.2 Qualitative data analysis

Responses to open-ended survey questions were analyzed using thematic coding to identify recurring compliance barriers. The coding process categorized SME challenges into key themes, such as financial constraints, cybersecurity expertise gaps, and regulatory uncertainty. Content analysis was applied to detect patterns in how SMEs perceive NIS2 obligations and their ability to meet regulatory requirements. To enhance the robustness of findings, qualitative results were cross-referenced with quantitative data. This validation ensured consistency between self-reported compliance barriers and statistical trends observed in the survey results.

3.4.3 Validation and reliability measures

Several measures were implemented to ensure data reliability and mitigate biases. Outlier detection techniques were used to identify inconsistencies in survey responses. Sampling bias was minimized by employing a stratified sampling approach, ensuring balanced representation across different KRITIS sectors. To address potential response bias, survey questions were designed to avoid leading phrasing and provide balanced answer choices. Missing data was handled through imputation methods where necessary, ensuring the integrity of statistical analysis.

4 Results

This section presents the findings from the empirical survey and legal analysis, detailing SME compliance readiness across KRITIS sectors, identified compliance barriers, and statistical insights. The results focus on sector-specific compliance levels, key challenges in meeting NIS2 requirements, and correlations between SME characteristics and cybersecurity preparedness.

4.1 Impact of company size on NIS2 compliance and interpretation

Company size plays a crucial role in determining how well organizations comply with the NIS2 Directive. Larger organizations generally have more resources, dedicated cybersecurity teams, and legal expertise to meet regulatory requirements, whereas smaller companies face significant challenges due to limited financial and technical

capacity.

Table 1 presents the self-reported compliance levels with NIS2 cybersecurity requirements across companies of different sizes. The mean compliance score across all companies was 63.1, with a standard deviation of 20.82, indicating moderate confidence in meeting the directive's standards. Smaller companies (<50 employees) reported lower compliance scores ranging between 25 and 55, while medium to large companies (>50 employees) reported higher scores between 70 and 95.

Table 1: Company Size and Compliance with NIS2 Cybersecurity Requirements (n=27)

Company Size	Mean	Standard Deviation	Score Range
All Companies	63.1	20.82	-
Small Companies (<50)	-	-	25 - 55
Medium to Large (>50)	-	-	70 - 95

Interpreting and implementing NIS2 legal requirements also poses challenges that vary by company size. Table 2 shows the average difficulty ratings assigned by respondents. The overall mean difficulty score was 71.55, with a standard deviation of 23.24, indicating that many companies struggle with the directive's complexity. Small companies reported the highest difficulty scores (80–100), suggesting a lack of specialized legal and compliance teams, while medium to large companies reported somewhat lower difficulty scores (50–70), reflecting access to greater legal resources.

Table 2: Difficulty in Interpreting and Implementing NIS2 Requirements (n=27)

Company Size	Mean	Standard Deviation	Score Range
All Companies	71.55	23.24	-
Small Companies (<50)	-	-	80 - 100
Medium to Large (>50)	-	-	50 - 70

Confidence in incident reporting under NIS2 varies significantly across organizations. Table 3 presents the findings on how companies assess their ability to meet the directive's strict reporting timelines. The overall mean confidence score was 54.8, with a high standard deviation of 38.46, reflecting diverse levels of preparedness. Small companies reported significantly lower confidence scores (20–60), whereas medium to large companies demonstrated much higher confidence (75–100), suggesting that well-established reporting protocols play a key role in compliance.

Table 3: Confidence in Incident Reporting (n=27)

Company Size	Mean	Standard Deviation	Score Range
All Companies	54.8	38.46	-
Small Companies (<50)	-	-	20 - 60
Medium to Large (>50)	-	-	75 - 100

4.2 Industry-specific challenges in NIS2 compliance

Industry sector plays a crucial role in shaping organizations' compliance levels and perceptions of regulatory challenges. Sectors such as telecommunications and IT, which have a history of cybersecurity regulation, tend to demonstrate higher compliance scores, while service-based sectors report lower readiness. Table 4 shows the

compliance readiness of companies in different industries.

Table 4: NIS2 Compliance Readiness by Industry Sector (n=27)

Industry Sector	Mean	Standard Deviation
Telecommunications & IT	80	7.5
Energy and Critical Infrastructure	70	15
Service-based Sectors	40-60	25

The difficulty of interpreting and implementing NIS2 requirements varies significantly across industries. Table 5 presents the reported difficulty levels. Companies in service-based sectors reported the highest difficulty ratings (mean 85), whereas IT and telecommunications companies reported lower scores (mean 60), suggesting they are better equipped to handle regulatory complexities.

Table 5: Difficulty in Interpreting NIS2 Requirements by Industry (n=27)

Industry Sector	Mean	Standard Deviation
Telecommunications & IT	60	15
Energy and Critical Infrastructure	75	20
Service-based Sectors	85	18

Confidence in incident reporting also differs by industry. Table 6 shows that telecommunications and IT companies reported the highest confidence scores (mean 90), while service-based industries reported the lowest confidence levels (mean 40), reflecting a lack of structured incident management processes.

Table 6: Confidence in Incident Reporting by Industry (n=27)

Industry Sector	Mean	Standard Deviation
Telecommunications & IT	90	10
Energy and Critical Infrastructure	70	25
Service-based Sectors	40	30

4.3 Compliance readiness across KRITIS sectors

Survey responses indicate variations in NIS2 compliance readiness among SMEs in different KRITIS sectors. Mean compliance scores were calculated to assess familiarity with NIS2 requirements, the implementation of cybersecurity measures, and the ability to meet reporting obligations.

Table 7: Mean Compliance Scores by KRITIS Sector (n=27)

Sector	Mean Compliance Score	Standard Deviation
Energy	72.3	12.1
Healthcare	65.8	10.9
Transportation	58.4	14.3
Finance	74.1	11.5
Digital Services	61.7	13.2

The compliance levels vary across sectors, with finance and energy reporting the highest readiness, while transportation and digital services exhibit lower preparedness.

4.4 Identified compliance barriers

Survey participants reported multiple obstacles in meeting NIS2 requirements. The most frequently cited barriers include financial constraints, technical limitations, and regulatory complexity.

Table 8: Most Commonly Reported Compliance Barriers (n=27)

Barrier	Percentage of SMEs Affected	Sectoral Variation
Budget constraints	78%	Higher in healthcare, transportation
Lack of cybersecurity expertise	64%	Higher in digital services
Regulatory complexity	59%	Evenly distributed across sectors
Unclear risk management guidelines	48%	Higher in small enterprises
Incident reporting burden	42%	Higher in finance and energy

4.5 Compliance gaps and regulatory intent

The NIS2 Directive aims to enhance cybersecurity across all critical infrastructure sectors, yet the data indicates a disparity between regulatory expectations and SME capabilities. Compliance readiness varies significantly by sector, reflecting differences in resource availability and cybersecurity maturity. Many SMEs struggle with risk management requirements and incident reporting obligations, suggesting that the regulatory framework does not fully account for the structural limitations of smaller enterprises. The challenges identified in the survey indicate that SMEs may require additional support mechanisms to bridge the gap between regulatory intent and practical implementation.

4.6 Qualitative insights on SME compliance with NIS2

The research included qualitative responses from SMEs in critical infrastructure sectors, providing a detailed perspective on compliance challenges, technological needs, and policy support mechanisms. These insights complement the statistical analysis by highlighting specific difficulties that SMEs encounter when implementing NIS2 requirements.

4.6.1 Key NIS2 requirements for SMEs in critical infrastructure sectors

SMEs in critical infrastructure sectors must comply with key provisions of the NIS2 Directive to enhance cybersecurity resilience. The most relevant requirements identified in the qualitative responses include incident reporting, risk management, supply chain security, and business continuity.

Incident reporting obligations are considered one of the most challenging aspects of compliance. SMEs operating in sectors such as energy, telecommunications, and finance rely on real-time operational systems, making rapid incident detection and reporting essential to prevent cascading disruptions. Respondents indicate that establishing clear reporting mechanisms and ensuring compliance with strict timelines pose significant difficulties, particularly for smaller firms with limited cybersecurity teams.

Risk management frameworks require SMEs to identify and mitigate cybersecurity risks that could impact critical services. Survey responses suggest that many SMEs struggle to implement comprehensive risk management due to limited technical expertise. Respondents indicate that sector-specific guidance and standardized risk assessment templates would improve compliance efficiency.

Supply chain security presents another major challenge, as many SMEs depend on third-

party vendors for software, hardware, and managed services. The NIS2 Directive mandates that businesses assess cybersecurity risks associated with external suppliers and implement mitigation strategies. SMEs report difficulties in enforcing security requirements for vendors, especially when dealing with larger suppliers that may not provide transparency regarding their security practices.

Business continuity and resilience requirements focus on maintaining operational functionality despite cyber incidents. SMEs acknowledge the importance of continuity planning but highlight difficulties in developing and testing incident response procedures. Many respondents emphasize the need for practical guidelines on implementing resilience measures tailored to SME resource limitations.

4.6.2 Challenges SMEs face in implementing NIS2

Survey responses reveal several major barriers that SMEs encounter when attempting to comply with the NIS2 Directive. These include resource constraints, lack of cybersecurity expertise, cybersecurity maturity limitations, and financial burdens.

Resource constraints are a recurrent issue across all critical infrastructure sectors. SMEs report that implementing cybersecurity measures requires investments in security tools, personnel training, and compliance monitoring systems, all of which may be financially unfeasible without external support. Respondents indicate that government incentives or industry-led support mechanisms could alleviate some of these costs.

Lack of cybersecurity expertise remains one of the most significant barriers to compliance. Many SMEs do not employ dedicated cybersecurity personnel, making it difficult to interpret regulatory obligations and implement effective security measures. The qualitative responses highlight that SMEs often rely on external consultants or managed security service providers to fill this gap. Respondents suggest that simplified compliance frameworks or advisory services would assist SMEs in aligning with NIS2 expectations.

Cybersecurity maturity varies significantly between industries, with SMEs in energy and finance sectors demonstrating higher levels of preparedness compared to those in transportation and digital services. SMEs operating legacy systems, particularly in healthcare and industrial control environments, report difficulties in upgrading security infrastructure to meet NIS2 standards. Respondents emphasize that compliance frameworks should account for the realities of integrating cybersecurity measures into legacy IT systems.

Financial burdens associated with NIS2 implementation create significant compliance challenges. SMEs report that upgrading network infrastructures, deploying AI-driven threat detection systems, and meeting incident reporting requirements require substantial investment. Respondents highlight that without financial subsidies or structured cost-sharing mechanisms, smaller firms may struggle to allocate the necessary resources for compliance.

4.6.3 Technologies and processes to support SMEs in NIS2 compliance

Survey participants provided insights into technologies and processes that could facilitate SME compliance with NIS2. Several approaches emerged as critical for improving cybersecurity readiness, including AI-driven security solutions, cloud-based

security platforms, Security Information and Event Management (SIEM) systems, automated compliance tools, and standardized cybersecurity frameworks.

AI-driven security solutions enable SMEs to automate threat detection, incident response, and compliance monitoring. Respondents note that AI-based systems reduce manual workload and enhance security event detection in real time. AI-driven compliance automation tools assist SMEs in adhering to NIS2 reporting obligations by streamlining data collection and submission processes.

Cloud-based security platforms offer SMEs cost-effective cybersecurity protection. Survey responses indicate that cloud security providers often integrate compliance features that help SMEs manage risk assessment, access controls, and data protection measures aligned with NIS2 requirements.

SIEM systems allow SMEs to centralize security monitoring and event correlation, providing a more structured approach to threat detection and response. Qualitative responses highlight that SMEs with limited IT staff benefit from SIEM systems by automating cybersecurity event analysis and supporting regulatory reporting requirements.

Automated compliance tools provide SMEs with pre-configured regulatory templates, security assessment frameworks, and real-time compliance tracking dashboards. Respondents emphasize that compliance automation tools reduce administrative burdens and improve regulatory adherence.

Standardized cybersecurity frameworks, such as ISO 27001 and NIST, serve as reference models for SMEs in structuring their cybersecurity strategies. Survey responses indicate that adopting recognized frameworks improves regulatory alignment and provides clear guidelines for risk management, incident response, and security governance.

4.6.4 Policy measures to facilitate SME compliance with NIS2

Survey respondents identified several policy measures that could help SMEs comply with NIS2 without creating excessive financial or operational burdens. These include financial subsidies, simplified compliance guidance, cybersecurity advisory services, public-private partnerships, and workforce training programs.

Financial subsidies and tax incentives could assist SMEs in offsetting the costs associated with cybersecurity investments. Respondents suggest that direct financial assistance for implementing security measures, such as AI-driven threat detection systems, network monitoring tools, and incident reporting infrastructure, would significantly improve SME compliance rates.

Simplified compliance guides tailored to SMEs would enhance regulatory understanding. Respondents indicate that breaking down NIS2 requirements into clear, actionable steps would facilitate implementation, especially for SMEs with limited legal and technical expertise.

Cybersecurity advisory services would provide SMEs with expert guidance on NIS2 compliance strategies. Survey responses emphasize that government-led or industry-supported advisory programs could bridge knowledge gaps and support SMEs in interpreting regulatory obligations.

Public-private partnerships could facilitate SME access to shared cybersecurity resources, such as best practice frameworks, compliance tools, and sector-specific risk assessment methodologies. Respondents high- light that collaborative initiatives between regulatory authorities and private industry would enhance SME cybersecurity resilience.

Free training and awareness programs could strengthen SME cybersecurity knowledge and improve work- force preparedness. Respondents stress that targeted cybersecurity education initiatives tailored to SME needs would help businesses integrate security best practices into daily operations.

4.6.5 Sector-specific compliance barriers

Sectoral variations in compliance readiness suggest that some industries are more equipped to meet NIS2 requirements than others. SMEs in finance and energy sectors report higher compliance scores, potentially due to pre-existing regulatory requirements and established cybersecurity infrastructures. SMEs in transportation and digital services exhibit lower readiness levels, citing limited financial and technical resources as primary obstacles. The results indicate that regulatory compliance is more difficult for SMEs that lack dedicated cybersecurity personnel or sector-specific guidance on implementing NIS2 obligations.

The survey responses highlight that financial constraints are the most frequently reported barrier to compliance. Many SMEs indicate that implementing NIS2 requirements would require substantial investment in security infrastructure and personnel training, costs that smaller firms cannot easily absorb. The shortage of cybersecurity expertise further complicates compliance, as SMEs often lack in-house specialists capable of managing regulatory requirements. Regulatory complexity remains a concern, with many SMEs reporting difficulties in interpreting risk management guidelines and understanding incident reporting procedures.

4.6.6 Policy and practical implications

The findings underscore the need for policy adjustments that account for SME-specific challenges. Regulatory compliance frameworks should differentiate between larger enterprises and SMEs, offering proportionate requirements that reflect available resources. Financial support mechanisms, such as government grants or tax incentives, could help alleviate the cost burden of implementing cybersecurity measures. Advisory services and sector-specific guidance would also assist SMEs in navigating NIS2 compliance requirements.

Compliance burdens could negatively impact SME innovation and competitiveness. High compliance costs and administrative complexity may divert resources away from business development, particularly in sectors with lower cybersecurity maturity. Policymakers should consider developing streamlined reporting procedures and simplified risk assessment frameworks to reduce the administrative burden on SMEs. Strengthening industry collaboration and knowledge-sharing initiatives may also improve SME cybersecurity resilience without imposing excessive costs.

5 Conclusions

This study examined the challenges that Small and Medium-sized Enterprises (SMEs) face in complying with the NIS2 Directive within Germany's critical infrastructure sectors. The findings indicate sectorial disparities in compliance readiness, with SMEs in finance and energy sectors reporting higher preparedness, while those in transportation and digital services exhibit lower levels of compliance. These differences result from variations in cybersecurity maturity, resource availability, and regulatory awareness.

The analysis identified financial constraints as a significant obstacle to compliance, particularly for SMEs operating with limited budgets. The absence of dedicated cybersecurity teams further complicates efforts to meet regulatory requirements, as many SMEs lack the expertise required to implement effective security measures. Regulatory complexity also emerged as a barrier, with SMEs struggling to interpret and apply NIS2 obligations in a way that aligns with their operational capabilities.

5.1 Policy and business recommendations

The findings suggest that SMEs require tailored regulatory support to comply with NIS2 obligations effectively. Compliance frameworks should differentiate between large enterprises and SMEs, ensuring that cybersecurity requirements remain proportional to available resources. Financial incentives, such as tax reliefs or government grants, could mitigate the financial burden of compliance. Advisory services and sector-specific guidance should be expanded to assist SMEs in implementing cybersecurity measures.

Simplification of reporting requirements and the provision of standardized risk assessment templates would improve compliance efficiency. Greater collaboration between regulatory bodies and industry stake- holders may enhance SME awareness and preparedness for cybersecurity regulations. Strengthening knowledge-sharing initiatives and cross-industry partnerships could facilitate best practice adoption among SMEs.

5.2 Broader implications for SME cybersecurity

SME cybersecurity resilience is essential for maintaining national security, as vulnerabilities in smaller enterprises can impact broader supply chains and critical infrastructure. Compliance with NIS2 is not only a regulatory obligation but also a strategic necessity for SMEs to remain competitive in an increasingly digitalized economy. Excessive compliance burdens may divert resources away from innovation and business growth. Policymakers must balance the enforcement of cybersecurity regulations with the economic feasibility of SME operations.

5.3 Comparison with existing literature on NIS2 compliance for SMEs in critical infrastructure sectors

Existing research on cybersecurity challenges for SMEs in critical infrastructure sectors highlights key issues relevant to NIS2 compliance. The literature indicates that SMEs are often overlooked in cybersecurity studies, which predominantly focus on large enterprises. This study confirms that SMEs face unique constraints that require further examination.

Much of the research on cybersecurity regulation centers on enterprise-level implementation, with limited attention given to how SMEs balance cybersecurity

challenges with resource constraints. The literature suggests that SMEs in critical infrastructure sectors require a deeper, multi-perspective exploration. Existing studies indicate that cybersecurity decision-making in SMEs varies depending on the stakeholder involved. Business owners prioritise operational concerns, while IT teams focus on security measures, leading to fragmented approaches to compliance. The findings from this study align with this observation, as SMEs in critical infrastructure sectors lack the expertise and resources to coordinate internal teams and external vendors effectively.

The balance between internal motivations and external regulatory demands presents another challenge. The literature identifies difficulties in reconciling ethical responsibility, trust, and perceived vulnerability with regulatory compliance, evolving cyber threats, and industry expectations. Research does not fully explore how SMEs manage these competing factors or how financial constraints influence their ability to adopt cybersecurity measures. This study supports the literature's conclusions, demonstrating that SMEs in critical infrastructure sectors struggle with financial constraints and operational challenges that hinder full compliance with NIS2.

Cybersecurity frameworks tailored to SMEs remain largely undeveloped. The literature suggests that existing frameworks, such as ISO 27001 and NIST, are too complex and resource-intensive for SMEs. This study finds that SMEs in critical infrastructure sectors encounter similar difficulties, particularly in meeting NIS2 requirements related to incident reporting and supply chain security.

5.4 NIS2 and its challenges for SMEs

The introduction of NIS2 has expanded the scope of cybersecurity requirements for SMEs, particularly in critical infrastructure sectors. The directive imposes stricter measures and introduces new compliance obligations, including mandatory incident reporting and supply chain security. Existing research acknowledges that NIS2 has increased compliance demands for SMEs but does not fully address the challenges specific to critical sectors. This study identifies cybersecurity expertise shortages, financial pressures, and operational limitations as significant barriers to NIS2 implementation.

Implementation gaps remain in addressing data security, AI-driven threats, and supply chain vulnerabilities. The literature recognises that NIS2 requires companies to assess supply chain security, but many SMEs lack the frameworks to manage third-party risks effectively. The findings confirm that SMEs in critical infrastructure sectors struggle with supply chain vulnerabilities, particularly when third-party vendors are involved.

5.5 Future research directions

Further research should examine how SMEs implement third-party risk management strategies under NIS2. The development of AI-based security solutions for detecting vulnerabilities in supply chains requires additional study. Financial strategies that enable SMEs to address both internal and external cybersecurity pressures need further exploration, particularly in relation to financial subsidies and simplified compliance guides. Research should also assess the long-term impact of NIS2 on SME

cybersecurity resilience, with comparative analyses across EU member states providing insights into best practices.

5.6 Final statement

Regulatory frameworks must accommodate the financial and operational realities of SMEs. Future research should evaluate the effectiveness of policy interventions aimed at supporting SMEs in meeting NIS2 requirements. Comparative analyses with other EU member states could offer additional perspectives on best practices for SME cybersecurity regulation.

Ensuring SME compliance with NIS2 requires coordinated efforts between regulators, industry stake- holders, and SMEs themselves. A balanced approach to cybersecurity regulation will strengthen resilience in critical infrastructure sectors while fostering an environment where SMEs can maintain robust security measures without compromising business viability.

References

[1]. European Commission. NIS2 directive: Strengthening Europe's cyber resilience. 2022 [cited 2025 Mar 12]. Available from: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[2]. Cisco. Wie aus NIS2-Herausforderungen strategische Chancen werden können. 2024.

[3]. Fernandez De Arroyabe I, Arranz CFA, Arroyabe MF, et al. Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Comput Secur*. 2023;124:102954. doi:10.1016/j.cose.2022.102954.

[4]. Arroyabe I, de Arroyabe J. The severity and effects of cyber-breaches in SMEs: A machine learning approach. *Enterp Inf Syst*. 2021;1–27.

[5]. Benz M, Chatterjee D. Calculated risk? A cybersecurity evaluation tool for SMEs. *Bus Horiz*. 2020;63(4):531–40. doi:10.1016/j.bushor.2020.03.010.

[6]. Gordon LA, Loeb MP. The economics of information security investment. *ACM Trans Inf Syst Secur*. 2002;5(4):438–57. doi:10.1145/581271.581274.

[7]. Fiorito R, Kollintzas T. Public goods, merit goods, and the relation between private and government consumption. *Eur Econ Rev*. 2004;48(6):1367–97. doi:10.1016/j.euroecorev.2003.10.006.

[8]. Ver Eecke W. Ethical dimensions of the economy: Making use of public goods. *Springer*. 2008. doi:10.1007/978-3-540-79572-0.

[9]. Talesh SA. Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. *Law Soc Inq*. 2018;43(2):417–40. doi:10.1111/lsi.12311.

[10]. Acquisti A, Taylor C, Wagman L. The economics of privacy. *J Econ Lit*. 2016;54(2):442–92. doi:10.1257/jel.54.2.442.

[11]. Lee J, Shin D. Machine learning for enterprises: Applications, algorithm selection, and challenges. *Bus Horiz*. 2020;63(2):157–70. doi:10.1016/j.bushor.2019.10.005.

[12]. Li Y. The impact of the GDPR on global technology development. *J Glob Inf Technol Manag*. 2019;22(1):1–6. doi:10.1080/1097198X.2019.1569186.

[13]. Tikkinen-Piri C, Rohunen A, Markkula J. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Comput Law Secur Rev*. 2018;34(1):134–53. doi:10.1016/j.clsr.2017.05.017.
[14]. Cavoukian A. Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario. 2010 [cited 2025 Mar 12]. Available from: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.
[15]. Grant Thornton. NIS-2 poses new challenges for German SMEs. 2024 [cited 2025 Mar 12]. Available from: https://www.grantthornton.de/en/insights/2024/nis-2-poses-new-challenges-for-german-smes/.
[16]. B2B Cyber Security. NIS2 directive: Objectives and challenges in implementation. 2024 [cited 2025 Mar 12]. Available from: https://b2b-cyber-security.de/en/nis2-directive-objectives-and-challenges-in-implementation/.
[17]. Reed Smith LLP. NIS2 implementation in Germany: Legal uncertainties and challenges. 2025 [cited 2025 Mar 12]. Available from: https://viewpoints.reedsmith.com/post/102jxuw/nis2-implementation-in-germany-failed.
[18]. Daoud MM, Serag AA. A proposed framework for studying the impact of cybersecurity on accounting information to increase trust in the financial reports in the context of Industry 4.0: An event, impact and response approach. *J Commer Finance*. 2022;42(1):20–61.
[19]. van Haastrecht M, van der Kleij R, Hoonhout J. Cybersecurity adoption in SMEs: The role of stakeholder awareness. *Cybersecurity J*. 2021;5(2):123–37.
[20]. Bada M, Nurse JR. Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Inf Comput Secur*. 2019;27(3):393–410.
[21]. Alahmari A, Duncan B. Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *IEEE CyberSA*. 2020. doi:10.1109/CyberSA49311.2020.9139638.
[22]. Perozzo L, Sturari M, Ferrari P. Cybersecurity challenges for SMEs: Limitations of existing standards and practical alternatives. *Int J Inf Secur*. 2022;14(3):289–303. doi:10.1007/s10207-022-00590-7.
[23]. Taeihagh A, Lim HSM. Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transp Rev*. 2019;39(1):103–28. doi:10.1080/01441647.2018.1494640.
[24]. Hoong C, Rezania D. Cybersecurity policy frameworks for SMEs: Strengthening global resilience. *J Cybersecur Policy*. 2024;11(1):45–63. doi:10.1080/23742917.2024.1950238.
[25]. Boswell R. 60% of European SMEs that are cyber-attacked have to close after six months. Startup Mag. 2023 [cited 2025 Mar 12]. Available from: https://startupsmagazine.co.uk/article-60-european-smes-are-cyber-attacked-have-close-after-six-months.
[26]. Choo KKR. The cyber threat landscape: Challenges and future research directions. *Comput Secur*. 2011;30(8):719–31. doi:10.1016/j.cose.2011.08.004.
[27]. Markopoulou D, Papakonstantinou V, De Hert P. The new EU cybersecurity framework: The NIS directive, ENISA's role and the General Data Protection Regulation. *Comput Law Secur Rev*. 2019;35(6):105336. doi:10.1016/j.clsr.2019.06.007.

[28]. European Union Agency for Cybersecurity (ENISA). Cybersecurity threats and recommendations for the NIS directive. 2023 [cited 2025 Mar 12]. Available from: https://www.enisa.europa.eu/publications.
[29]. EU-Lex. Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2 directive). 2025 [cited 2025 Mar 12]. Available from: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.
[30]. European Commission. Proposal for a regulation of the European Parliament and the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the network of national coordination centres. 2025.
[31]. Hepke J, Lanzrath F. Cybersecurity compliance challenges for SMEs under the NIS2 directive. *J Inf Secur Policy*. 2024;18(1):45–63. doi:10.1080/23742917.2024.1950238.