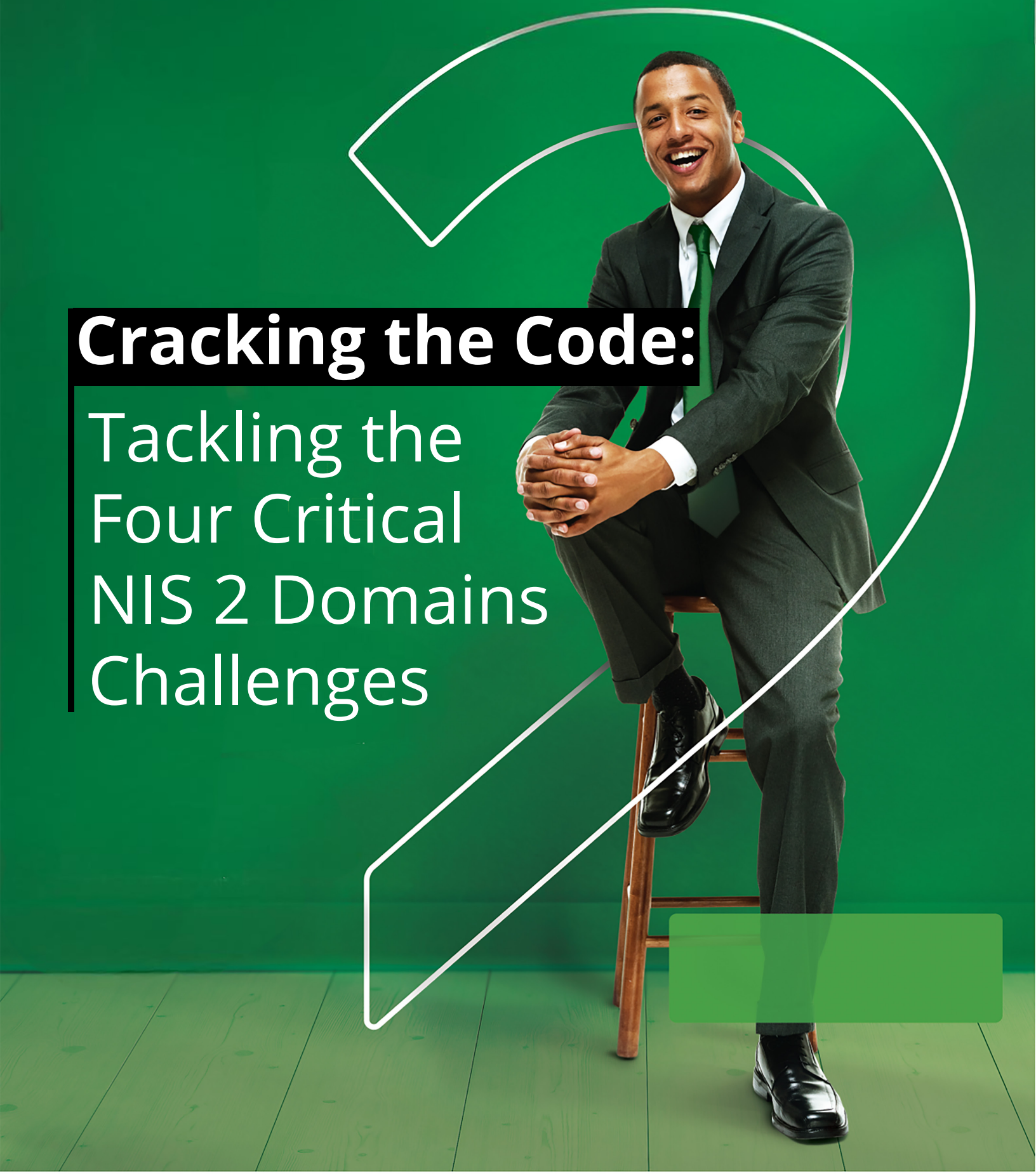
ISC2

ISC2 Standards and Practice



Cracking the Code:

Tackling the Four Critical NIS 2 Domains Challenges

EXECUTIVE SUMMARY

The Directive on Security of Network and Information Systems[1] (NIS 2 Directive), proposed in December 2020, strengthens the European Union's (EU's) cybersecurity framework, extending its scope to broaden essential and critical sectors to comply with requirements. All member states were required to implement the NIS 2 Directive by October 17, 2024. However, as of November 2024, nearly a quarter of the EU member states[2]— Belgium, Italy, Latvia, Lithuania, Hungary, and Croatia—have made significant progress by adopting the NIS 2 Directive into their national laws. Most EU member states are still in the process of preparing to meet its requirements.

DOCUMENT PURPOSE

With the support of member professionals, ISC2 developed this guide to meet the needs of medium-sized organizations, particularly those with limited resources and understaffed teams affected by the NIS 2 Directive. This resource provides practical strategies and insights from cybersecurity professionals to help organizations focus on the most critical compliance tasks.

Although this guide is not a complete manual for NIS 2 Directive compliance, it does share the lessons learned by ISC2 volunteer subject matter experts (SMEs) to support the journey toward compliance.

[1] NIS – Network and Information Systems, NIS 2 Directive. Official Journal of the European Union. 14 December 2022. Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.
[2] "NIS 2: Where are European countries in transposing the directive?" Wavestone. 21 November 2024. Source: https://www.wavestone.com/en/insight/nis-2-european-countries-transposing-directive.

SCOPE OF GUIDANCE AND PRELIMINARY FINDINGS

This guide tackles the four critical challenge domains commonly encountered by SMEs when preparing for and implementing the NIS 2 Directive:

1. **Regulatory and Legal Compliance**
    a. Governance and Leadership
    b. Scope Expansion[3]
    c. Harmonization[4]
2. **Risk Management and Incident Reporting**
3. **Supply Chain and Third-Party Security**
4. **Resource Optimization**

Governance and Leadership, Scope Expansion, and Harmonization are topics under the Regulatory and Legal Compliance domain, as one of four key domains covered in this document.

SUMMARY OF CRITICAL CHALLENGES AND FINDINGS

ISC2 surveyed more than 70 volunteer SMEs from various sectors, such as Information and Communication Technology (ICT) services, transportation, financial, and energy industries, all revealing similar challenges in the survey results. SMEs' pressing concerns include leadership's lack of awareness about personal liability, pending clarifications from local authorities, and organizations' resource limitations; they consistently voiced these commonly faced challenges in their responses.

Specifically, ISC2's volunteer SMEs shared their proven strategies, such as engaging leadership regularly, establishing a strong accountability plan, reviewing existing implemented frameworks

[3] Scope expansion refers to the broader and more inclusive scope of the NIS 2 Directive compared to the previous NIS Directive (2016/1148).
[4] Harmonization itself is not a challenge for the end user or organization. We refer to the challenges under the Harmonization category (e.g., pending clarification from local authorities).

such as the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27001 or the EU's Digital Operational Resilience Act (DORA),[5] and leveraging publicly available resources. These strategies enabled them to navigate the NIS 2 Directive compliance journey effectively.

UNIQUE VALUE PROPOSITION

With the support of more than 70 ISC2 member SMEs, we collectively analyzed, prioritized, and combined over 350 hours' worth of expert ideas. Such a powerful and agnostic data source allows us to share insightful and valuable peer-to-peer opinions.

METHODOLOGY

ISC2 employed a structured approach, shown in Figure 1, to develop this NIS 2 Directive implementation strategies guide.

Figure 1 Methodology overview for NIS 2 Directive implementation strategies guidance

These steps outline how we gathered SME insights and approaches for overcoming challenges:

1. First, we designed customized questionnaires to survey SMEs from various industries across the globe, targeted to identify their most pressing challenges.

[5] DORA. The Digital Operational Resilience Act (DORA) is an EU regulation that entered into force on 16 January 2023 and will apply as of 17 January 2025. Source: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora.

2. Subsequently, we developed detailed worksheets to document real-life, insightful solutions provided by experienced SMEs.
3. Through in-depth workshop discussions with selected NIS 2 Directive experts, we gathered solution-driven worksheets addressing four critical challenge domains.

This methodology enabled us to accurately identify critical concerns and provide actionable, insightful solutions to address them effectively.

TARGET AUDIENCE, APPLICABILITY, AND LIMITATIONS

Target audience: Our target audience consists of cybersecurity professionals, compliance officers, and organizational leaders within medium-sized organizations[6] across various sectors that must comply with the NIS 2 Directive requirements.

Key focus areas: This guide addresses the most commonly encountered challenges identified during the NIS 2 Directive implementation process, as determined by SMEs in the ISC2 surveys. The guide offers practical, actionable strategies to help organizations tackle these challenges effectively.

Geographical applicability: This guide is intended for medium-sized[7] EU-based or multinational organizations providing services to the EU member states' markets, as the NIS 2 Directive applies to essential and important entities within specific sectors, rather than all European organizations.

Limitations: Though this guide provides practical strategies to help organizations begin the NIS 2 Directive implementation process, it does not serve as a comprehensive guide for achieving complete compliance. To fully comply, consult with accredited legal professionals as well as credentialed cybersecurity experts with recognized certifications such as ISC2's Certified

[6] According to NIS 2 Directive, Chapter 1, Article 3, medium-sized enterprises are defined as those having fewer than 250 employees and either an annual turnover not exceeding €50 million or an annual balance sheet total not exceeding €43 million.
[7] The NIS 2 Directive scope is not restricted only to medium-sized organizations. It applies to large organizations by default, as well as medium-sized ones in specific circumstances, such as those operating in critical sectors or providing key services.

Information Systems Security Professional (CISSP) and Certified Cloud Security Professional (CCSP). Appendix A describes additional roles and relevant certifications.

BEST PRACTICES

This section highlights actionable strategies to help organizations initiate and navigate their NIS 2 Directive compliance journey.

The recommendations are based on collective feedback from ISC2 SMEs with real-world experience implementing NIS 2 compliance. Figure 2 shows the challenges they encounter most frequently

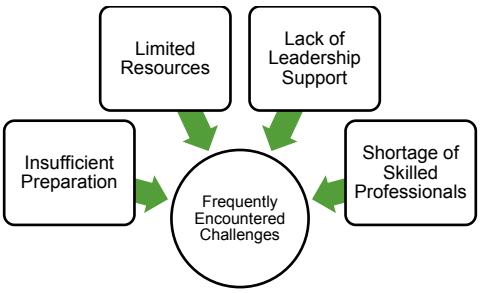


Figure 2 Challenges SMEs encounter most frequently

GOVERNANCE AND LEADERSHIP

Governance and leadership are crucial for NIS 2 Directive compliance, emphasizing accountability, risk management, and strategic alignment. Chapter 4[8] highlights board-level responsibility and personal liability, ensuring senior management's active engagement.

Governance aligns cybersecurity strategies with business goals, while leadership fosters a security-first culture and ensures clarity in roles. This is important for addressing NIS 2 Directive's requirements, such as incident reporting, risk mitigation, and resource allocation.

[8] NIS 2 Directive, Chapter 4, “Cybersecurity risk management measures and reporting obligations.” Source: https://eur-lex.europa.eu/eli/dir/2022/2555.

Leaders oversee policy approval, resource allocation, and compliance monitoring, while governance promotes collaboration and preparedness. They drive accountability, proactive risk management, and resilience, forming the foundation for NIS 2 Directive compliance and organizational security.

Key Challenges

Following feedback and discussions, the SME group identified several key challenges relating to Governance and Leadership that may delay or hinder the successful implementation of the NIS 2 Directive within organizations.

While the causes of these challenges are varied, ISC2 SMEs frequently cite a lack of leadership awareness and competing organizational priorities as significant factors. The identified challenges follow:

- **Personal liability unawareness:** Senior management and key stakeholders in multinational companies operating within the EU must comply with the NIS 2 Directive, which imposes accountability and personal liability for non-compliance.
- **Competing priorities**: Organizational priorities often overshadow the need to address NIS 2 Directive compliance, resulting in delays or neglect in implementing necessary measures.
- **Resource constraints:** Leadership's focus on revenue generation over cybersecurity investment poses a significant challenge.
- **Budget battles:** Competing internal funding priorities create additional obstacles for cybersecurity professionals seeking resources to ensure NIS 2 Directive compliance.

These challenges underscore the need for enhanced education and advocacy to ensure organizational alignment and proactive compliance.

Recommended Strategies to Address Challenges

The following fundamental approaches can be effectively implemented by those preparing to develop their NIS 2 Directive implementation plans:

- **Ensure leadership awareness:** Foster a comprehensive understanding among leadership of compliance implications, including personal liability, to enhance decision-making and support.

- **Collaborate across teams:** Work with other teams or personnel facing similar compliance funding demands to present a unified front, strengthening the case for management support.
- **Translate technical jargon:** Make compliance communication accessible by translating technical terms into business-focused language that aligns with executive priorities.
- **Engage leadership effectively:** Dedicate adequate time for discussions and engagement with leadership to ensure alignment, clarity, and commitment.
- **Establish an accountability framework:** Create a robust governance structure with clearly defined roles and responsibilities to enhance accountability and streamline decision-making.

These actionable strategies from the ISC2 SMEs should be promoted across the cybersecurity community.

SCOPE EXPANSION

Compared to NIS 1, NIS 2 significantly expands its scope of application to include new sectors[9] and industries. Specifically, NIS 2 requires organizations to adopt new roles, skills, and qualifications for cybersecurity. Adapting to additional extensive cybersecurity requirements and duties can burden many small or medium-sized organizations.

KEY CHALLENGES

The following challenges highlight the need for technical, organizational, and cultural strategies, as they can help organizations manage the expanded scope of the NIS 2 Directive and make a smoother transition from physical to digital safety.

- **Overwhelming compliance demands:** Organizations struggle to manage the increase in cybersecurity and compliance demands due to NIS 2 Directive's expanded scope.

[9] Not only are new sectors included, but the criteria has also been lowered so that more organizations are now within the "scope."

- **Cultural and strategic adjustments:** Business sectors such as transportation traditionally prioritized operational and passengers' physical safety over cyber safety; the addition of cybersecurity safety represents significant cultural and strategic adjustments.

RECOMMENDED STRATEGIES TO ADDRESS CHALLENGES

While addressing the challenges posed by increased cybersecurity requirements, we should also recognize the evolving threats to our industries and the necessity of these requirements to safeguard our communities.

According to German digital association Bitkom e. V., in 2022 analog and digital threats caused damages of €203 billion, rising to €266 billion in 2024.[10] The impact of increased automation, AI advancements, and collaboration among attacker groups has escalated significantly in recent years. Companies remain underprepared, prompting legislators to push public institutions and businesses to enhance protections, especially for critical infrastructure. For that purpose, the German government's draft law on NIS 2 implementation aims to achieve a high cybersecurity standard across the EU.

Even organizations outside the NIS 2 Directive's scope should proactively address its requirements to strengthen their cybersecurity in a manner suited to their needs.

- **Addressing overwhelming compliance demands' challenges:** Since many NIS 2 Directive requirements aren't new, organizations should compare existing measures with NIS 2 and adjust as needed. Expanding management systems like ISO 9001[11] to include key Information Security Management System (ISMS) components can help integrate

[10] "Cybercrime and sabotage cost German firms $300 bln in past year." Reuters. 24 August 2024. Source: https://www.reuters.com/technology/cybersecurity/cybercrime-sabotage-cost-german-firms-300-bln-past-year-2024-08-28.
[11] ISO 9001 is a quality management system (QMS). When combined with key ISMS components, it becomes ISO 27001.

information security, allowing organizations to use existing processes for NIS 2 Directive compliance.

- **Addressing cultural and strategic adjustment challenges:** Cyber professionals in the transport sector, such as railway transportation, should raise awareness and align cybersecurity investments with the company's focus on safety and service reliability.

HARMONIZATION

The NIS 2 Directive aims to align and harmonize the cybersecurity legislative framework across EU member states. However, the interpretation and implementation of the NIS 2 Directive may differ significantly among them. EU member states have the flexibility to adopt variations from the EU-wide requirements, which can create challenges for organizations as they await clarification on national regulations.

KEY CHALLENGES

These challenges demand achieving clarity while maintaining persistence throughout the compliance process:

- **Pending clarification:** One of the top challenges organizations face is waiting for the clarification of country-specific implementations.
- **Penalty fatigue:** While the NIS 2 Directive strengthens the cybersecurity legislative framework and increases personal liability for non-compliance,[12] some leadership teams may not perceive the risk of non-compliance as critically high. This could be due to “penalty fatigue” or “regulatory apathy,” when an organization becomes desensitized to risk after repeated violations or due to governing bodies failing to enforce fines.

[12] NIS 2 Directive, Chapter 4, Article 20(1), “Governance.” Source: https://eur-lex.europa.eu/eli/dir/2022/2555.

RECOMMENDED STRATEGIES TO ADDRESS CHALLENGES

Pending clarification: The following strategies are recommended to navigate the waiting period for country-specific implementation:

- In the early implementation stages, key experts, such as data protection/privacy and legal specialists, should be involved to clarify compatibility with the organization's mission objectives.
- Proactively communicate with and seek advice from local authorities and expert groups.
- For organizations subject to other regulatory requirements (e.g., DORA), avoid duplicated NIS 2 Directive efforts.
- Internal communications, especially with senior management, should begin with establishing NIS 2 Directive requirements as early as possible. SMEs have reported underestimating the time, human, and financial resources needed, so it is strongly recommended that sufficient resources be allocated for each.

Penalty fatigue: The following strategies are recommended to increase awareness of personal and organizational impacts from non-compliance if enforced properly, regardless of past enforcement activities:

- Leadership needs to understand they are *personally* responsible[13] for an organization's cybersecurity compliance, not government or law enforcement agencies. Their role primarily involves defense and investigative activities.
- Organizational cybersecurity should be seen as a key responsibility of an organization's leadership, not the duty of external authorities to manage. European lawmakers

[13] Article 20(3) NIS 2 Directive – This includes being temporarily banned from holding managerial positions within the organization.

emphasize cybersecurity as a management issue, meaning it's up to executive leadership to prioritize it.

- Leadership teams can be held ultimately responsible, although they can request appropriate support from law enforcement or government agencies when necessary.

RISK MANAGEMENT FRAMEWORKS AND INCIDENT REPORTING

The NIS 2 Directive distinguishes between risk management frameworks and incident reporting, with risk management outlined in Chapter 2 and incident reporting covered in Chapter 4.[14] These areas are addressed here, as they form an integrated strategy for mitigating cybersecurity risks and ensuring prompt, structured incident responses critical to NIS 2 compliance.

Articles 21 and 22[15] require essential entities and critical infrastructure operators to implement appropriate technical, organizational, and operational measures to manage cybersecurity risks. These measures include the development of policies for risk analysis, information system security, incident management, and supply chain security.

The most frequently cited challenge regarding this domain was "unpreparedness for compliance," where organizations were unready to meet the NIS 2 Directive's security measures, including incident reporting requirements. This was followed by challenges in building and enhancing security measures to achieve compliance.

[14] NIS 2 Directive, Chapter 2, "Coordinated cybersecurity frameworks," and Chapter 4, "Cybersecurity risk management measures and reporting obligations." Source: https://eur-lex.europa.eu/eli/dir/2022/2555.
[15] NIS 2 Directive, Chapter 4, Article 21, "Cybersecurity risk management measures," and Article 22, "Union level coordinated security risk assessments of critical supply chains." Source: https://eur-lex.europa.eu/eli/dir/2022/2555.

Regarding incident reporting requirements, Article 23[16] further strengthens these requirements by mandating early detection and reporting mechanisms, including a strict 24-hour deadline for reporting cybersecurity incidents to the National Competent Authority (NCA).[17]

The NCA reviews and verifies the incident and must inform the relative national Computer Security Incident Response Team (CSIRT) as soon as possible to facilitate coordination, as shown in Figure 3. NIS 2 Directive's Article 23, Paragraph 8, CSIRT and NCAs must share relevant information with other affected EU member states to address cross-border impacts accordingly.

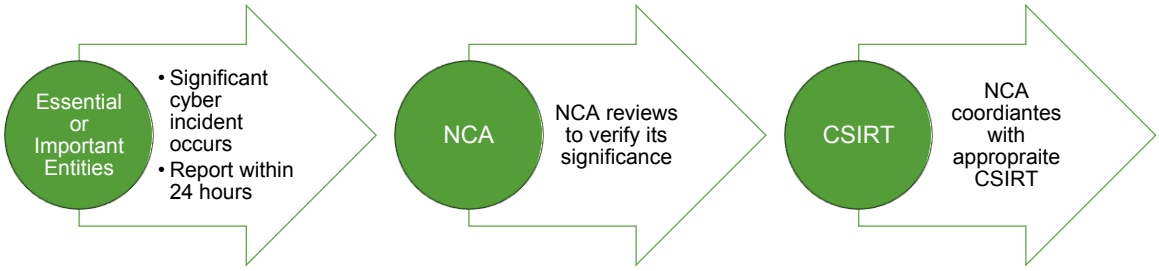


Figure 3 EU member state reporting obligations. Source: NIS 2 Directive, Article 23, Paragraph1-8.

ISO/IEC 27001

As a result of the similar reporting structure within ISO/IEC 27001, those who have already implemented the requirements of the standard will find it easier to adopt and accept NIS 2 Directive incident reporting requirements.

[16] NIS 2 Directive, Chapter 4, Article 23, "Reporting obligations." Source: https://eur-lex.europa.eu/eli/dir/2022/2555.
[17] NCA – National Competent Authority: The NCA is the primary authority designated by an EU Member State to oversee the implementation and enforcement of the NIS 2 Directive within its jurisdiction.

Key Challenges

The following top challenges were identified:

- **Unpreparedness:** Many organizations were found to be unprepared for NIS 2 Directive requirements, with minimal cybersecurity frameworks and weak incident response and reporting processes. The lack of established protocols and unclear compliance concepts makes meeting the NIS 2 Directive's expectations difficult.
- **Security measures:** Developing and improving security measures to meet NIS 2 Directive compliance requirements remains a significant hurdle for many organizations, especially those lacking in financial resources and/or sufficiently trained people.
- **Incident response and reporting:** Organizations face significant challenges in managing effective incident responses within the tight timeframes mandated by NIS 2 Directive. The NIS 2 Directive's enhanced reporting obligations include the reporting of significant cyber incidents within 24 hours. This is particularly demanding for entities lacking a mature incident response plan (IRP).

These challenges highlight the need for robust frameworks, efficient coordination, and resource allocation to achieve compliance with the NIS 2 Directive.

Recommended Strategies to Address Challenges

- **Addressing unpreparedness:**
  - Raise leadership awareness of NIS 2 Directive compliance and the risks of non-compliance, including personal and organizational liability. Secure leadership buy-in through a top-down approach to access funding and initiate a concerted effort to address all issues.
  - Establish a dedicated team for responsibility and compliance. Formalizing incident response, investing in continuous monitoring, and implementing real-time threat alerting are good practices
  - Finally, compliance should be sustained throughout normal business-as-usual activities.
- **Addressing security measures:**
  - Conduct a gap analysis and prioritize tasks for effective resource allocation. A cybersecurity maturity assessment can be used to evaluate the level of maturity for cybersecurity initiatives, while industry certifications like ISO 27001can help organizations align with the NIS 2 Directive.

- Clear metrics enable ongoing evaluation, and demonstrating positive results motivates continued management investment, ensuring sustained compliance and improvement.

- **Addressing incident response:**
  - Reporting can be challenging for complex organizations. Those already-compliant regulatory frameworks (e.g., DORA, Cyber Resilience Act [CRA], etc.) may find alignment with the reporting requirements of NIS 2 Directive more readily attainable. However, creating an initial incident reporting mechanism will involve addressing at least three essential factors to comply with the NIS 2 Directive:
    - Defining clear roles and requirements, such as the responsibilities for sending reports to authorities and ensuring appropriate feedback is communicated with all stakeholders.
    - Developing a mutual understanding of the requirements and the ramifications before implementation of the incident response process.
    - Communicating and seeking advice from authorities, the NCA, national CSIRT, and local expert groups within the industry.

SUPPLY CHAIN AND THIRD-PARTY SECURITY

Article 21 (“Cybersecurity Risk Management Measures”) and Article 23 (“Reporting Obligations”) list the details of supply chain security obligations and supply chain-related incident reporting requirements, respectively.

NIS 2 Directive introduces supply chain security requirements to ensure that essential and critical service operators assess and manage risks associated with their direct vendors and service providers. Most of the requirements shown in Figure 4 are covered in articles 14 and 21 through 23,[18] from identifying supply chain risks to developing a holistic supply chain strategy.

[18] NIS 2 Directive, Chapter 3, Article 14, “Cooperation group”; Chapter 4, Article 21, “Cybersecurity risk management measures,“ Article 22, “Union level coordinated security risk assessments of critical supply chains,” and Article 23 “Reporting obligations.” Source: https://eur-lex.europa.eu/eli/dir/2022/2555.

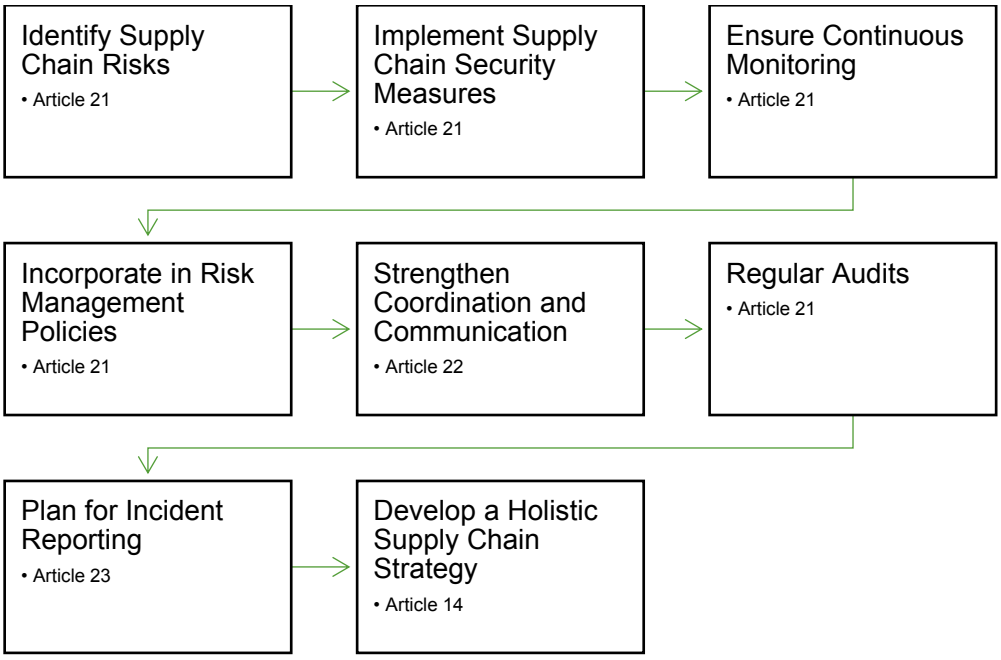


Figure 4 NIS 2 Directive requirements from articles 14 and 21–23

To summarize, identifying supply chain risks and implementing security measures will constitute the initial phase of meeting NIS 2 Directive compliance requirements. Based on feedback from our ISC2 volunteer SMEs, these steps are also the most challenging part of the process. The reasons lie in the organizational unpreparedness and readiness issues, particularly for understaffed medium-sized organizations, and the lack of funding to invest in the necessary threat monitoring and detection tools.

KEY CHALLENGES

We highlight the following key supply chain challenges:

- **Aligning third-party risk assessment processes:**
  - Aligning third-party vendors' risk assessments with NIS 2 Directive supply chain requirements is challenging. Identifying all suppliers and maintaining regular updates alongside internal audits is time-consuming.
  - Vendors or suppliers of security infrastructure components may fail to fully disclose information regarding downstream products due to proprietary or regulatory limitations.
  - Establishing an effective onboarding process and ongoing monitoring of new suppliers adds complexity.
- **Ensuring suppliers meet NIS 2 Directive requirements:**

- A common challenge for organizations is ensuring their suppliers are NIS 2 Directive compliant, especially when suppliers are unaware of or reluctant to meet the requirements. Noncompliant suppliers can also risk the organization's NIS 2 Directive compliance.

RECOMMENDED STRATEGIES TO ADDRESS CHALLENGES

- **Addressing third-party risk assessment process challenges:**
  - Establishing an asset repository to identify critical suppliers is essential, similar to the process outlined in Article 28 of the General Data Protection Regulation (GDPR).[19] Once identified, evaluate suppliers thoroughly and agree on service details in the service-level agreement (SLA) contracts, covering service purpose, data type, and security measures.
  - Tools like the information security assessment (minimum asset table) can be used to gauge supplier security maturity. Encourage non-compliant suppliers to improve through contractual measures or reconsider cooperation if maturity goals are unmet.
  - Organizations with complex facilities, like power plants or energy suppliers, often rely on multiple service providers for operations, from design to billing. Identifying critical infrastructure asset management is key to identifying all direct suppliers and service providers.
  - A detailed asset inventory offers a valuable overview of assets and providers. The positive aspect is that some suppliers, especially those offering ICT-based equipment, already meet NIS 2 Directive supply chain security requirements.
- **Addressing suppliers' NIS 2 Directive compliance status challenge:**
  - Understanding the regulatory requirements that organizations should comply with and identifying relevant third-party vendors is essential. Once identified, organizations should assess their suppliers' compliance status using the following example questions:
    - How does my organization assess these third-party vendors' compliance with NIS 2 Directive and my organization's regulatory requirements? This needs to be reassessed throughout the project.

[19] General Data Protection Regulation (GDPR), Article 28, “Processor.” Source: https://gdpr-text.com/read/article-28.

- Do third-party vendors understand their obligations and (where relevant) commit to compliance through their service terms or contracts?
- What is my organization's go/no-go criteria for doing business with a supplier? When would we walk away?
- How does the vendor distinguish critical infrastructure, and how does that affect delivery of my product?

Organizations should create questionnaires to assess supplier compliance, using the above questions as examples. The goal is to gather enough information to mitigate the risk of NIS 2 Directive non-compliance.

Sometimes, critical vendors may resist due diligence activities. Incorporating relevant regulatory requirements and the vendors' roles in NIS 2 Directive compliance into the contract terms is essential.

RESOURCE OPTIMIZATION

KEY CHALLENGES

As the NIS 2 Directive becomes local law in some EU member states, others are expected to follow imminently. According to a recent report,[20] many organizations affected by the NIS 2 Directive are either underprepared or entirely unprepared to meet the new compliance requirements.

These organizations have had to reallocate funds from critical areas like risk management, recruitment, and crisis management. To help resource-constrained organizations, our ISC2 volunteer SMEs assessed their needs, prioritized them, and developed practical strategies to support medium-sized organizations beginning their NIS 2 Directive compliance journey.

[20] Bremmer, M., CSO, "NIS 2 compliance eats up IT budgets despite doubts." 1 November 2024. Source: https://www.csoonline.com/article/3596485/NIS 2-compliance-eats-up-it-budgets-despite-doubts.html.

RECOMMENDED STRATEGIES TO ADDRESS CHALLENGES

Understanding resource constraints:

1. We should first understand our resource constraints to address budget challenges. Affected organizations should evaluate constraints through the lens of expertise and governance domains.
2. Once these constraints are identified, we can conduct a gap assessment using any existing framework, such as ISO 27001, Trusted Information Security Assessment Exchange (TISAX) for the auto industry in Germany, or the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Organizations may consider using an iterative approach to close the gap in the initial phase rather than closing it entirely in one attempt.
3. Taking the iterative approach to moving toward compliance in several steps could optimize the cost and enhance a greater chance of success. Especially for specific technical requirements, organizations may adopt a proportionality approach instead of a complete, all-at-once implementation.
4. This scenario allows organizations more time to prioritize imminent requirements while strategically road-mapping the remaining tasks. Additionally, this approach helps organizations identify areas suitable for outsourcing versus those that should remain in-house.

Cost-optimizing strategies: For resource-constrained organizations, several practical strategies can optimize the cost of implementing NIS 2 Directive compliances; these include but are not limited to:

1. **Budget allocation and roles accountability:** Leadership should assign NIS 2 Directive compliance accountability at the C-level, understanding the consequences of non-compliance. This should lead to a risk assessment that informs strategic budget allocations, potentially using frameworks like ISO 27001 and advancing to models like TISAX or NIST CSF.
2. **Leveraging external support:**
    a. Organizations may conduct a thorough cost-benefit analysis (CBA) to evaluate if outsourcing some tasks is more cost-effective than performing in-house. However, it is essential to emphasize that organizations should only delegate tasks, not the accountability for NIS 2 Directive compliance.

b. Organizations should thoroughly assess the implications of risk ownership and regulatory compliance before outsourcing the tasks.

3. **Build a scalable compliance strategy:** Organizations can start with established cybersecurity practices, like ISO/IEC 27001, map them to NIS 2 Directive requirements to identify overlaps and gaps, then address them to achieve full NIS 2 Directive compliance.
4. **Leveraging existing resources:**
    a. Several available resources, such as the NIST CSF, can help organizations achieve NIS 2 Directive compliance by providing cybersecurity frameworks, references, and recommendations.
    b. Additional references can be found in the Appendix B.

CONCLUSION

We strongly recommend organizations invest time and resources to thoroughly explore the details of NIS 2 Directive compliance requirements, as NIS 2 Directive implementation, interpretation, and legislative requirements can differ slightly according to local and national laws. Therefore, organizations should engage with local authoritative bodies, cooperation groups, and consulting firms to provide detailed local compliance requirements as early as possible.

Furthermore, NIS 2 Directive compliance is an ongoing process, not a one-time task. Our volunteer experts advise peers to start planning as soon as possible, engage the leadership team and inform them of the severe penalties for non-compliance, define clear team roles, and build strong cyber frameworks to avoid unnecessary mistakes encountered by our expert volunteers. Appendix C provides a set of checklists for tackling NIS 2 Directive compliance.

APPENDIX A

ISC2 CERTIFICATIONS RELEVANT TO NIS 2 DIRECTIVE IMPLEMENTATION

ISC2 offers a range of certifications aligned with the skills and knowledge required for compliance with the NIS 2 Directive. These certifications cover key cybersecurity, risk management, and governance areas, all essential for meeting NIS 2 Directive requirements.

CISSP (Certified Information Systems Security Professional)

CISSP is a widely recognized certification in the cybersecurity field, covering a broad spectrum of topics such as security and risk management, asset security, and security operations, all of which are crucial for NIS 2 Directive compliance.

CCSP (Certified Cloud Security Professional)

As more organizations move to the cloud, CCSP offers in-depth knowledge of cloud security architecture, design, and operations, ensuring that cloud deployments align with NIS 2 Directive requirements.

CGRC (Certified in Governance, Risk, and Compliance)

CGRC focuses on governance, risk management, and compliance. This certification helps professionals understand how to manage and authorize information systems within risk management frameworks, directly supporting NIS 2's Directive compliance mandates.

SSCP (Systems Security Certified Practitioner)

SSCP is designed for IT administrators and network security professionals, covering critical areas such as access controls, security operations, and incident response, which are essential for implementing the technical requirements of the NIS 2 Directive.

HCISPP (HealthCare Information Security and Privacy Practitioner)

HCISPP is specifically aimed at the healthcare sector, providing knowledge on securing sensitive healthcare data and information systems, aligning with sector-specific requirements under NIS 2 Directive.

Source: https://www.isc2.org/certifications

APPENDIX B

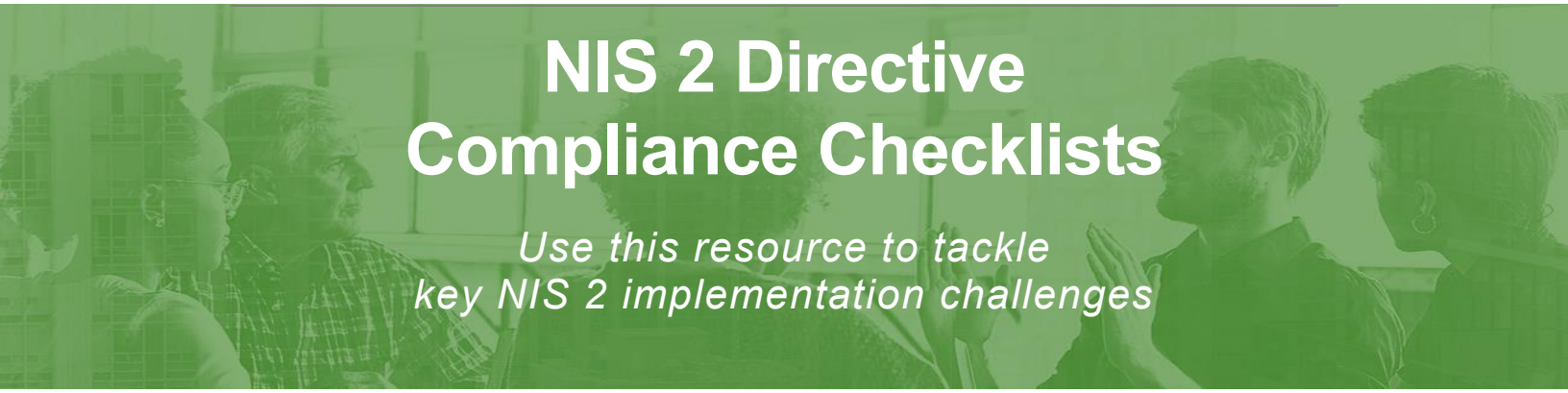
LEVERAGE EXISTING RESOURCES

1. IT-Grundschutz Methodology (guidance for implementing robust information security based on BSI standards): https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
2. TISAX resources and downloads: https://portal.enx.com/en-us/TISAX/downloads/
3. Secure Controls Framework (comprehensive framework for managing cybersecurity and privacy controls): https://securecontrolsframework.com
4. NIST CSF: https://www.nist.gov/cyberframework
5. Cloud Controls Matrix (CCM) (Cloud Security Alliance matrix for cloud security risk management): https://cloudsecurityalliance.org/research/cloud-controls-matrix
6. OWASP Cheat Sheet Series (essential security practices for developers and cybersecurity professionals): https://cheatsheetseries.owasp.org
7. Cyber Essentials Self-Assessment Guide (IASME Consortium's guide to the Cyber Essentials certification): https://iasme.co.uk/cyber-essentials/free-download-of-self-assessment-questions
8. Exercise in a Box Overview (NCSC's free tool for simulating cyber incidents and testing response plans): https://www.ncsc.gov.uk/section/exercise-in-a-box/overview/

APPENDIX C

CHECKLISTS FOR CRACKING THE CODE

Use the compliance checklists on the following pages as a resource to tackle key NIS 2 implementation challenges.



NIS 2 Directive Compliance Checklists

Use this resource to tackle key NIS 2 implementation challenges

KEY CHALLENGE: GOVERNANCE AND LEADERSHIP

Strategy	Recommended Actions	
Collaborate across teams	Work with other teams or roles facing similar compliance funding demands to present a unified front, strengthening the case for management support.	☐
Translate technical jargon	Make compliance communication accessible by translating technical terms into business-focused language that aligns with executive priorities.	☐
Use metaphors for clarity	Employ simple metaphors, such as T-shirt sizes, to explain technical complexities. For instance, categorize tasks from "XS" (policy writing) to "XL" (incident reporting mechanisms).	☐
Ensure leadership awareness	Foster a comprehensive understanding among the leadership of compliance implications, including personal liability, to enhance decision-making and support.	☐
Engage leadership effectively	Dedicate adequate time for discussions and engagement with leadership to ensure alignment, clarity, and commitment.	☐
Establish an accountability framework	Create a robust governance structure with clearly defined roles and responsibilities to enhance accountability and streamline decision-making.	☐

KEY CHALLENGE: SCOPE EXPANSION

Strategy	Recommended Actions	
Expand management systems	Compare existing measures with NIS 2 Directive and adjust as needed. Expanding management systems like ISO 9001 to include key ISMS components can help integrate information security, allowing organizations to use existing processes for NIS 2 Directive compliance.	☐
Identify cultural and strategic opportunities	Raise awareness and align cybersecurity investments with the company's focus on safety and service reliability. Balancing NIS 2 Directive compliance with minimal disruption to services is key, and a phased approach could help achieve this.	☐

KEY CHALLENGE: HARMONIZATION

Strategy	Recommended Actions	
Be proactive during the waiting period for country-specific implementation	Involve key experts, such as data protection/privacy and legal specialists, early in the implementation stages.	☐
	Proactively communicate with and seek advice from local authorities and expert groups.	☐
	Avoid duplicated DORA and NIS 2 Directive efforts (if applicable to the organization).	☐
	Begin internal communications regarding NIS 2 Directive requirements, especially with senior management, as early as possible.	☐
Reduce penalty fatigue by raising awareness and gaining buy-in	Communicate clearly and regularly with key stakeholders about their responsibility.	☐
	Help business owners and managers recognize that they are *personally* responsible for cybersecurity. It's not just the government or law enforcement's job—they ensure their organizations are secure.	☐
	Promote cybersecurity as a key responsibility of the organization's management, not something for outside authorities to manage. European lawmakers stress that cybersecurity is a management issue, meaning it's up to leadership to prioritize it.	☐
	Reinforce accountability of the leadership team and their ultimate responsibility, even though they can request support from law enforcement or government agencies.	☐

KEY CHALLENGE: RISK MANAGEMENT AND INCIDENT REPORTING

Strategy	Recommended Actions	
Mitigate unpreparedness	Raise leadership awareness of NIS 2 Directive compliance and the risks of non-compliance, including personal and organizational liability. Secure leadership buy-in through a top-down approach to access funding and form a project team.	☐
	Establish a dedicated team for accountability and compliance to prioritize incident response and investment in tools for 24/7 monitoring and real-time threat alerts.	☐
	Integrate compliance into daily operations for sustainability.	☐
Highlight strategies for addressing compliance challenges	A key step is conducting a gap analysis and prioritizing tasks for effective resource allocation. Tools like a Cybersecurity Maturity Assessment can evaluate cybersecurity effectiveness, while certifications like ISO 27001 help align with the NIS 2 Directive.	☐
	Clear metrics enable ongoing evaluation, and demonstrating positive results motivates continued	☐

	management investment, ensuring sustained compliance and improvement.	
Effective incident response	Organizations already compliant with DORA (EU Regulation 2022/2554) may find aligning with the reporting requirements more manageable.	☐
	For those who are setting up an incident reporting mechanism from scratch, be sure to address at least three essential factors to comply with the NIS 2 Directive: • Define clear roles and system requirements, such as who will send the report to the authorities and who is responsible for the required information; ensure the current ticketing system can meet necessary reporting needs. • Establish a well-organized reporting system and provide awareness training to all staff. • Develop a mutual understanding of the requirements and the ramifications before implementation.	☐
	Communicate and seek advice from authorities, NCA, CSIRT, and local expert groups within the industry.	☐

KEY CHALLENGE: SUPPLY CHAIN AND THIRD-PARTY SECURITY

Strategy	Recommended Actions	
Implement third-party risk assessment processes	Establish an asset repository to identify critical suppliers, similar to the process outlined in Article 28 of the GDPR. Once identified, evaluate suppliers thoroughly and agree on service details in SLA contracts, covering service purpose, data type, and security measures.	☐
	Implement tools like the information security assessment to gauge supplier security maturity. Encourage non-compliant suppliers to improve through contractual measures or reconsider cooperation if maturity goals are unmet.	☐
	Organizations with complex facilities, like power plants or energy suppliers, often rely on multiple service providers for operations, from design to billing. Critical asset management is key to identifying all direct suppliers and service providers.	☐
	Create and maintain a detailed asset inventory, which provides a valuable overview of assets and providers.	☐
Assess suppliers' NIS 2 Directive compliance status	Understand the regulatory requirements that organizations should comply with and identify relevant third-party vendors.	☐
	Create questionnaires to assess supplier compliance, using the above questions as examples. The goal is to gather enough information to mitigate the risk of NIS 2 Directive non-compliance.	☐
	Critical vendors may resist due diligence activities. Incorporate relevant regulatory requirements and the vendors' roles in NIS 2 Directive compliance into the contract terms.	☐

	Once identified, assess supplier compliance status using the following example questions: • How does my organization assess these third-party vendors' compliance with NIS 2 Directive and my organization's regulatory requirements? • Do third-party vendors understand their obligations and (where relevant) commit to compliance through their service terms or contracts?	☐

KEY CHALLENGE: RESOURCE OPTIMIZATION

Strategy	Recommended Actions	
Understand resource constraints	Evaluate resource constraints through the lens of expertise and governance domains.	☐
	Conduct a gap assessment using any existing framework, such as ISO 27001, TISAX in Germany, or the NIST CSF. Prioritize imminent requirements while strategically road-mapping the remaining tasks.	☐
	Consider using an iterative approach to close the gap in the initial phase rather than closing it entirely in one attempt to optimize costs and enhance a greater chance of success.	☐
	Identify areas suitable for outsourcing versus those that should remain in-house.	☐
Budget allocation and roles accountability	Leadership should assign NIS 2 Directive compliance accountability at the C-level, understanding the consequences of non-compliance. This should lead to a risk assessment that informs strategic budget allocations, potentially using frameworks like ISO 27001 and advancing to models like TISAX or NIST CSF.	☐
Leveraging external support	Conduct a thorough cost-benefit analysis (CBA) to evaluate if outsourcing some tasks is more cost-effective than performing in-house. However, it is essential to emphasize that organizations should only delegate tasks, not the accountability for NIS 2 Directive compliance. Thoroughly assess the implications of risk ownership and regulatory compliance before outsourcing the tasks.	☐
Build a scalable compliance strategy	Start with established cybersecurity practices, like ISO/IEC 27001, map them to NIS 2 Directive requirements to identify overlaps and gaps, then address them to achieve full NIS 2 Directive compliance.	☐
Leveraging existing resources	Reference existing resources, like the NIST CSF, to achieve NIS 2 Directive compliance through cybersecurity frameworks, references, and recommendations. Additional information can be found in the appendix section.	☐

ISC2.org

ISC2™

Your Future. Secured.

625 N Washington Street,
Suite 400
Alexandria, VA 22314
United States

United Kingdom
info-emea@isc2.org

Level 20, ONE IFC,
1 Harbour View Street,
Central
Hong Kong S.A.R.
isc2asia@isc2.org