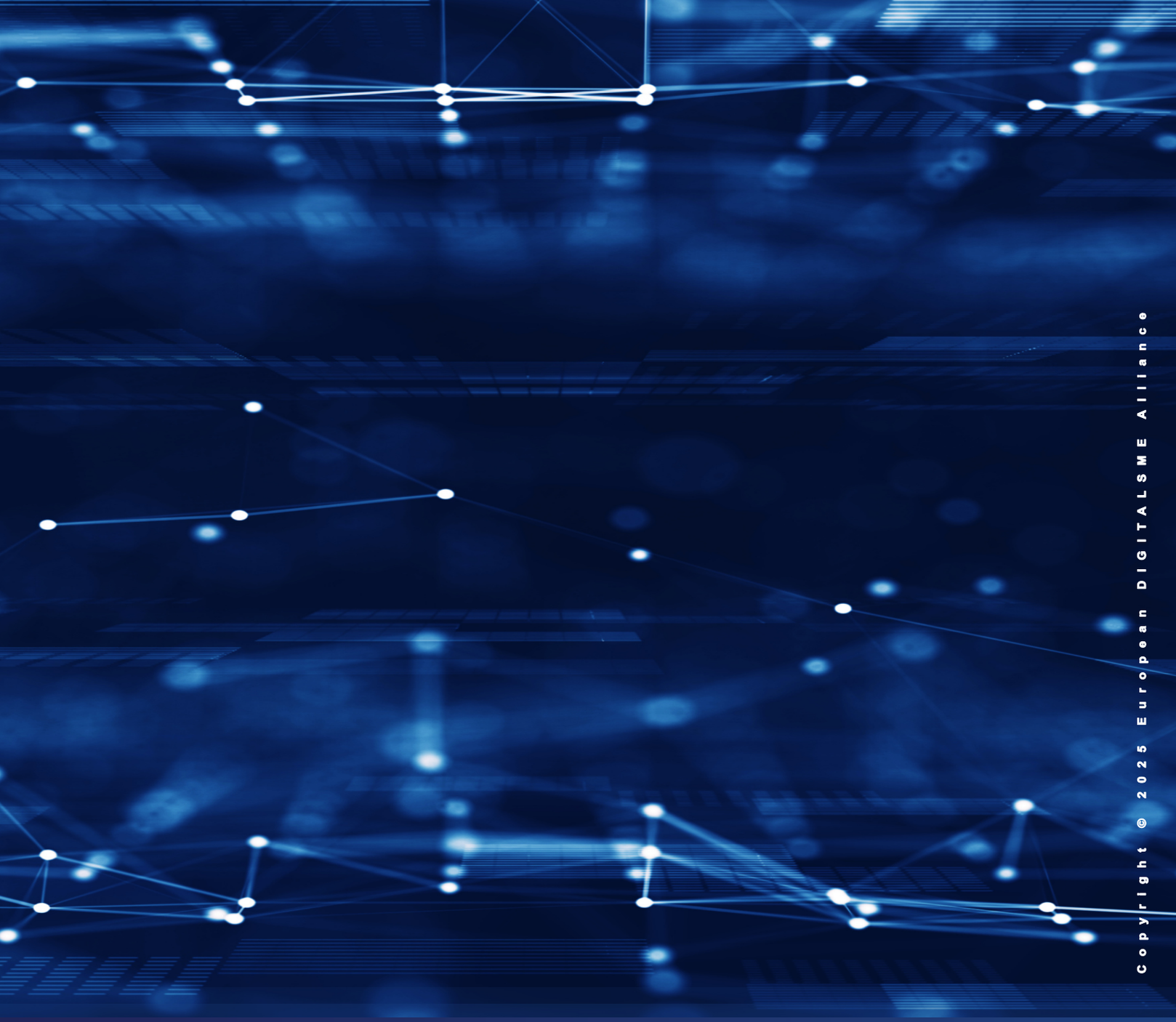

European DIGITAL SME Alliance

July 2025

A BLUEPRINT TO THE NETWORK AND INFORMATION SYSTEMS DIRECTIVE UPDATE (NIS2)

step-by-step guide for SMEs

CONTACT: T: +32 28930235 - E: office@digitalsme.eu ADDRESS: Rue Marie Thérèse 21 bte.5, 1000, Brussels, Belgium

Introduction

Authors

James Philpot

Davide Iaccarino

Stephan Schwichtenberg

Davide Giribaldi

Andrea Caccia

Daniele Tumietto

In today's digital age, the security and resilience of critical infrastructure and online services are paramount, not only for large corporations but also for small and medium-sized enterprises (SMEs) and citizens. With cyber threats becoming increasingly sophisticated and pervasive, regulatory measures like the Network and Information Systems (NIS) Directive play a crucial role in ensuring that vital digital assets are protected, and governments can ensure that companies have implemented adequate cybersecurity measures.

The NIS Directive, introduced by the European Union in 2016, aims to enhance the overall level of cybersecurity across member states. The original Directive set forth the first comprehensive set of cybersecurity regulations to improve the overall security of networks and information systems within the EU. Recently, an update to this directive was rolled out, bringing more stringent requirements and a broader scope.

For SMEs, understanding and complying with these updates is essential, not just to avoid potential fines and legal consequences, but also to build and maintain trust with their customers. While the Directive (with specific exceptions) exempts Small and Micro entities from the scope, Medium-sized businesses must comply with the requirements. Further to this, companies under the scope of the Directive will be obliged to ensure the cybersecurity of their supply chains; therefore, Small and Micro entities will still need to be aware of the requirements and the steps they can take to prove their cybersecurity, and new processes that will be required as part of the Directive.

Therefore, this guide is designed to help SMEs navigate the complexities of the NIS Directive update. It will break down the key components of the directive, highlight any specific obligations for your business, and help you understand and undertake actionable steps to achieve and demonstrate that you are a secure supplier and service provider.

TABLE OF CONTENTS

Chapter 1: What is the Network and Information Systems Directive and who does it apply to?

NIS2, or the Network and Information Systems Directive 2, is an updated version of the original NIS Directive (Directive on Security of Network and Information Systems), which the European Union (EU) implemented to enhance the cybersecurity of network and information systems across its member states.

Scope and Coverage

NIS2 significantly broadens the scope of the original directive to include more sectors and types of services. It covers sectors such as energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, and space.

Enhanced Requirements

The directive imposes stricter cybersecurity requirements on both essential and important entities, which include implementing risk management measures and reporting incidents to relevant authorities.

Incident Reporting

NIS2 mandates more stringent and standardised procedures for reporting significant incidents. Organizations must report incidents to their national competent authorities or Computer Security Incident Response Teams (CSIRTs) within 24 hours of detection.

Governance and Oversight

NIS2 introduces stronger supervisory measures, including the designation of national competent authorities responsible for overseeing and enforcing the directive. These authorities are empowered to conduct audits, require information, and impose penalties for non-compliance.

Supply Chain Security

The directive emphasises the importance of supply chain security by requiring entities to manage risks associated with their supply chain and service providers. The updated Directive allows for these provisions to be included in supplier's contracts.

The goal of NIS2 is to create a high common level of cybersecurity across the EU, protect critical infrastructure and essential services from cyber threats, and ensure the resilience of networks and information systems.

Does the NIS2 Directive Apply to Your Company?

The NIS2 applies to a range of different companies and sectors. This is wider than the original Directive as new sectors are now included in the scope. Below is a list of entities the Directive covers (including specific small and micro companies).

1. **Entities Covered by the NIS2 Directive Include:**

The directive categorizes entities into "essential" and "important" based on their significance to the economy and society.

Essential Entities typically include sectors such as:

- **Energy:** Electricity, oil, gas, and district heating and cooling.
- **Transport:** Air, rail, water, and road transport, including logistics.
- **Banking and Financial Market Infrastructures**
- **Health:** Healthcare providers, hospitals, and laboratories.
- **Drinking Water and Wastewater Management**
- **Digital Infrastructure:** Internet exchange points, Domain Name System qualified trust service providers, and cloud computing services.
- **Public Administration:** Central and regional government bodies.

Important Entities cover sectors like:

- **Postal and Courier Services**
- **Waste Management**
- **Manufacturing**: Production of critical products such as medical devices and pharmaceuticals.
- **Food Production and Distribution**
- **Space**: Operators providing space-based services.
- **Digital Infrastructure**: Providers of public electronic communications networks or services, trust services, or Domain Name System.

2. Medium and Large Organizations:

The directive primarily applies to medium—and large-sized organizations within the specified sectors based on criteria such as employee numbers and annual turnover.

Company category	Staff headcount	Turnover	OR Balance sheet total
Medium-sized	< 250	≤ € 50 m	≤ € 43 m
Small	< 50	≤ € 10 m	≤ € 10 m
Micro	< 10	≤ € 2 m	≤ € 2 m

3. Certain Small and Micro Entities:

While the focus is on larger organisations, it also applies to SMEs when they are providers of public electronic communications networks or services, trusts services or domain name system; some smaller entities may also fall under the directive if they are deemed critical for societal or economic activities, or if they are the sole provider of a service within a member state.

4. Digital Service Providers:

This includes online marketplaces, online search engines, and social networking services, recognising their integral role in modern society and the economy.

Below is a test to help companies determine if they are within the scope of the NIS2 Directive. It involves a series of questions that assess the nature of their operations, the sectors they operate in, and their specific functions.

NIS2 In-Scope Assessment

Size of company: Are you a micro/small enterprise or larger?

- Micro/small
- Medium or large

1. Sector Classification: Does your company operate in any of the following sectors?

- Energy (e.g., electricity, gas, oil)
- Transport (e.g., air, rail, water, road)
- Banking
- Financial Market Infrastructures
- Health (e.g., healthcare providers, hospitals)
- Drinking Water Supply and Distribution
- Wastewater Management
- Digital Infrastructure (e.g., data centres, cloud computing services)
- Public Administration
- Space (e.g., satellite operators)

  o Yes/No

2. Service Type:

Does your company provide essential services that are critical to the maintenance of societal and economic activities?

- Yes / No

Does your company provide public electronic communications networks or services, trust services, or domain name system?

3. Service Dependency:

Is your company a digital service provider, such as an online marketplace, online search engine, or cloud computing service?

- Yes / No

4. Impact Assessment

Would an incident affecting your company have a significant disruptive impact on essential services, public safety, or economic and social well-being?

- Yes / No

5. Geographical Reach:

Does your company operate across multiple EU member states?

- Yes / No

6. Supply Chain Involvement:

Is your company involved in the supply chain of critical infrastructure or essential services?

- Yes / No

7. Public Administration:

Is your company a part of the public administration or does it provide critical services to public administration entities?

- Yes / No

8. Incident History

Has your company experienced any cybersecurity incidents that had a significant impact on your services or operations in the past?

- Yes / No

If you answered "**Yes**" to any of the questions: Your company likely falls within the scope of the NIS2 Directive, and you should review the specific requirements and obligations that apply to your sector and services.

If you answered "**No**" to all questions, your company may not be covered by the NIS2 Directive. However, it is advisable to stay informed about cybersecurity regulations and best practices to ensure robust protection against cyber threats.

If you answered yes to any of the questions above **and** you are a medium-sized enterprise or larger, your company likely falls within the scope of the Directive. Even if you are a micro or small enterprise, under certain circumstances, the Directive may still apply to your company. Therefore, it is recommended that the scope of the Directive and its requirements be further reviewed to understand better how you are likely to be affected.

Chapter 2: What is obliged by NIS2? Overview of requirements and supply chain security

Building upon its predecessor (the original NIS Directive), NIS2 aims to set clearer and firmer requirements for organisations to increase their digital resilience. The 10 core cyber-measures outlined in Article 21, par. 2 of the Directive can be considered the foundation for organisations to comply with this Directive. These measures cover various areas, from governance and risk management to human resources security and cryptography. Understanding these requirements is essential to ensure a strong cybersecurity posture for your business.

1. Governance and Accountability

Organisations must establish strong cybersecurity governance, including assigning responsibilities to senior management and setting clear accountability for cybersecurity risks. This can be achieved by implementing a governance framework that ensures top management involvement in cybersecurity and clarifies roles and responsibilities for cybersecurity decisions.

2. Risk Management

Organisations must conduct regular risk assessments and implement security policies that must be tailored to the organisation's risk profile, covering threat identification and mitigation strategies. Using frameworks such as the one provided by ISO/IEC 27001 can facilitate risk assessments and ensure that cybersecurity policies address emerging threats and vulnerabilities.

3. Incident Management

NIS2 aims to ensure that organisations are equipped with an incident response plan that enables quick detection, management, and recovery from cyber incidents. It is necessary to pool resources within your organisation to create a response team and protocol for identifying, reporting, and mitigating incidents, including cooperation with NIS2 authorities for significant incidents.

4. Business Continuity

Under the Directive, critical business functions must continue in the face of cyber disruptions through continuity planning and crisis management. Organisations are now required to develop business continuity plans, backup systems, and crisis communication strategies to maintain operations during cyber incidents.

5. Supply Chain Security

NIS2 requires organisations to address security risks associated with third-party providers and partners to reduce vulnerabilities in the supply chain. Suppliers must be examined for cybersecurity compliance, integrate cybersecurity requirements in contracts, and conduct regular supplier audits. In this case, standards like ISO/IEC 27001 can help benchmark suppliers' cybersecurity posture.

6. Network and Information Systems Security

NIS2 focuses on integrating security into the lifecycle of IT systems, from development and acquisition to ongoing maintenance. Secure software development practices must be implemented as well as regular system updates and security testing to identify and resolve potential vulnerabilities early.

7. Cyber Hygiene

Organisations must integrate cybersecurity awareness into their work culture, making it a core aspect of daily operations and decision-making. By cultivating a workforce that is alert and cyber-aware about security risks, companies can enhance their resilience against cyber threats. It is necessary to provide regular cybersecurity training, phishing simulations, and guidance on secure behaviour, such as using strong passwords.

8. Human Resources Security

Organisations must address cybersecurity risks related to employees, contractors, and partners throughout their entire work lifecycle – from recruitment to offboarding. This measure aims to prevent insider threats and secure sensitive information. Tailored policies that include background checks, cybersecurity training for new hires, and access controls based on roles and responsibilities must be implemented.

9. Access Control

The Directive aims to restrict access to systems and data based on user roles and responsibilities, ensuring only authorised individuals can access sensitive information. Multi-factor authentication (MFA) is essential, as well as regular access reviews to limit and monitor access to critical systems and data.

10. Cryptography

Organisations must use cryptographic measures to protect the confidentiality, integrity, and security of data, especially when handling sensitive or personal information. Effective encryption minimises the risk of unauthorised access, both during data transfer and while

data is at rest. This can be achieved by implementing strong encryption protocols for data, ensuring that sensitive information remains protected from interception. Regular updates and cryptographic standard reviews are among the best practices to maintain strong protection against evolving threats.

One of the standout elements of NIS2 is its emphasis on supply chain security. Several cyber incidents originate from third-party providers. This means that a strong focus on securing the supply chain is critical for overall resilience. To meet NIS2 requirements, organisations should assess the cybersecurity practices of their vendors before engagement, ensuring that they are compliant with recognised standards such as ISO/IEC 27001. Contracts with third parties should clearly outline cybersecurity obligations, including incident notification timelines, access controls, and data protection measures. Regular audits are essential to confirm ongoing compliance, while threat intelligence tools help monitor potential risks across the supply chain. Strengthening supply chain security under NIS2 empowers organisations to build a unified front against cyber threats, promoting resilience across all interconnected partners.

Chapter 3: How to show you are a secure supplier?

NIS2 places significant importance on supply chain security, requiring suppliers to adopt stricter cybersecurity measures that safeguard not only their operations but also those of their clients and partners. What happens if you are a supplier? We will explore the essential steps suppliers can take to strengthen their security posture and meet NIS2 requirements to become trusted, resilient, and secured partners.

As a supplier, the table below will help you understand some of the shared security expectations between the Directive and an essential security standard: ISO/IEC 27001. Some specific services require compliance with specific standards, such as ETSI EN 319 401 for trust service providers. This guide does not give specific indications for such cases, but the following guidance on ISO/IEC 270001 can still provide relevant information.

For suppliers who are already ISO/IEC 27001 compliant, there is an opportunity to streamline efforts when meeting the NIS2 Directive requirements. This table highlights overlaps between the two frameworks, showing where your current ISO/IEC 27001 controls can support your compliance with NIS2. In both ISO/IEC 27001 and NIS2, a “control” is a requirement or guideline aimed at securing information, minimising risks, and ensuring business continuity. The areas highlighted in the table represent key aspects of supply chain security. This approach not only saves time but also increases your security practices, helping you align with NIS2 requirements and reinforce client trust without overhauling established processes. Through these overlapping controls, ISO/IEC 27001 compliance becomes a strong foundation for meeting NIS2 expectations. This allows you to expand compliance while supporting a resilient supply chain. The following comparison focuses on six major areas where ISO/IEC 27001 controls align with NIS2 requirements, showing where your current efforts already support compliance with both frameworks:

1. Risk Assessment & Management

Control Family	Control description	NIS2 Relations
ISO/IEC 27001 A.5.1	Policies for information security: information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Article 21, par. 2 (a) and Annex I, point 2: require entities to implement risk management frameworks that address security risks in network and information systems, including those posed by third parties.
ISO/IEC 27001 A.5.2	Information Security roles and responsibilities: organisations shall define and allocate information security roles and responsibilities according to the organisation's needs.	
ISO/IEC 27001 A.5.3	Segregation of Duties: conflicting duties and conflicting areas of responsibility shall be segregated.	
ISO/IEC 27001 A.5.4	Management responsibilities: management shall require all personnel to apply information security by the established information security policy, topic-specific policies and procedures of the organisation.	
ISO/IEC 27001 A.5.31	Legal, statutory, regulatory and contractual requirements: the organisation's approach to meet these requirements shall be identified, documented and kept up to date.	
ISO/IEC 27001 A.5.37	Documented operating procedures: operating procedures for information processing facilities shall be documented and made available to personnel who need them.	

Advice:

Suppliers must assess security risks in their supply chain, document identified risks and implement mitigation measures. This includes ensuring that critical roles within their organisation are clearly defined to prevent conflicts of interest and unauthorised access.

2. Security in Supplier Agreements

Control Family	Control description	NIS2 relations
ISO/IEC 27001 A.5.19	Information security in supplier relationships: processes and procedures shall be defined and implemented to manage the information security risks associated with the use of suppliers' products or services.	Article 21, par. 2 (d) and Annex I, point 6: require the inclusion of security requirements in supplier agreements to address data protection, handling, and incident response.
ISO/IEC 27001 A.5.20	Addressing information security within supplier agreements: relevant information security requirements shall be established and agreed upon with each supplier based on the type of supplier relationship.	
ISO/IEC 27001 A.5.21	Managing information security in the ICT supply chain: processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	
ISO/IEC 27001 A.5.22	Monitoring, review and change management of supplier services: the organisation shall regularly monitor, review, evaluate and manage changes in supplier information security practices and service delivery.	
ISO/IEC 27001 A.5.23	Information security for use of cloud services: processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organisation's information security requirements.	

Advice:

Suppliers should formalise security requirements in contracts, covering topics like data protection, access controls, and breach notification.

3. Incident Response & Notification

Control Family	Control Discription	NIS2 Relations
ISO/IEC 27001 A.5.24	Information security incident management planning and preparation: the organisation shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Article 21, par. 2 (b), Article 23 and Annex I, point 3.3: require entities to have incident response processes and report significant incidents to clients and authorities within specified timeframes.
ISO/IEC 27001 A.5.25	Assessment and decision on information security events: the organisation shall assess information security events and decide if they will be categorised as information security incidents.	
ISO/IEC 27001 A.5.26	Response to information security incidents: information security incidents shall be responded to in accordance with the documented procedures.	
ISO/IEC 27001 A.5.28	Collection of evidence: the organisation shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	
ISO/IEC 27001 A.6.8	Information security event reporting: the organisation shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels promptly.	
ISO/IEC 27001 A.8.15	Logging: logs that record activities, expectations, faults and other relevant events shall be products, stored, protected and analysed.	
ISO/IEC 27001 A.8.16	Monitoring activities: Networks, systems, and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	

Advice:

Suppliers must develop a detailed incident response plan, including timelines for notifying clients of breaches or security issues that may impact services.

4. Business Continuity & Resilience

Control Family	Control Discription	NIS2 Relations
ISO/IEC 27001 A.5.29	Information security during disruption: the organisation shall plan how to maintain information security at an appropriate level during disruption.	Article 21, par. 2 (c) and Annex I, point 4: require business continuity and disaster recovery plans to minimise service interruptions.
ISO/IEC 27001 A.5.30	ICT readiness for business continuity: ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	
ISO/IEC 27001 A.5.37	Documented operating procedures: operating procedures for information processing facilities shall be documented and made available to personnel who need them.	
ISO/IEC 27001 A.7.11	Supporting utilities: information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	
ISO/IEC 27001 A.8.13	Information backup: backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic specific policy on backup.	
ISO/IEC 27001 A.8.14	Redundancy of information processing facilities: information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	

Advice:

Suppliers should develop and regularly test business continuity plans, including backup and recovery strategies. These plans should account for dependencies on other vendors and include procedures for maintaining critical services during disruptions.

Free and Open-Source Software Suppliers

As a supplier of Free and Open-Source Software (FOSS), you are expected to implement risk management practices around every open-source library and dependency you use. Your customers will demand assurance that you conduct thorough risk assessments before integrating any open-source component. This means evaluating known vulnerabilities using tools such as Dependabot, Snyk, or OSS Index, assessing license risk to ensure compliance with customer policies, and verifying that dependencies are actively maintained. The outcomes of these assessments should be formally documented and shared with your customers, demonstrating that the FOSS supply chain you support is safe.

In addition to the initial risk assessment, continuous monitoring is essential. By leveraging automated vulnerability scanners and other security tools, you can track emerging risks in real time and swiftly address any issues. By involving yourself with the OSS community, you will reinforce the quality of your code but also provide your customers with confidence that you remain informed about the latest security threats. A comprehensive strategy for FOSS suppliers should include clear strategies for dependency management and licensing compliance. Practices such as digitally signing code commits and providing a Software Bill of Materials (SBOM) that details all dependencies and their security status are vital. Such transparency will assure that your customers are fully aware of the components in your software and the measures you take to keep them secure. Regular updates and a defined patch management process, where critical vulnerabilities are fixed within an acceptable timeframe, are also crucial. Subscribing to CVE databases and using automated tools to detect and mitigate risks before they are flagged by customers can further increase your security posture.

Contractual obligations play an important role. NIS2-compliant customers may require that your contracts include clauses mandating your support during security incidents, clear security guarantees about the FOSS software provided, and the right to audit your security practices. As a supplier, you should prepare a comprehensive compliance package that includes your risk management framework, incident response plan, and audit policies. By ensuring that your security controls are well documented and that you are prepared for potential audits, you not only meet requirements but also build lasting

trust with your customers.

CHECKLIST

- ☐ **Risk Assessment & Vulnerability Monitoring in open-source dependencies**
- ☐ **Documented Licensing & Compliance Policies (e.g., SPDX)**
- ☐ **Secure Development Lifecycle (SDLC), including code reviews & penetration testing**
- ☐ **Patch Management Policy with automated updates for FOSS dependencies**
- ☐ **Community Engagement & Peer Reviews as proof of secure FOSS contribution**
- ☐ **Contractual Readiness for security guarantees, audit rights, and incident response**

Chapter 4: Managing your security

Based on the above identification of controls and the requirements set out in the NIS2 Directive, it is possible to identify steps that you can take to ensure the security of your company and demonstrate your security to your clients.

1. Governance and Accountability

To establish effective cybersecurity governance and accountability, SMEs should formally assign roles and responsibilities for information security, taking into account the organisation's structure and culture. While smaller organisations may assign multiple roles to a single person or outsource some roles, top management cannot be outsourced.

Key roles and responsibilities include:

- **Top Management:** They are responsible for information security governance, ensuring it aligns with business goals, and understanding the value of critical assets to business operations.
- **Information Security Steering Committee**: A committee comprising stakeholders from main departments meets quarterly to address security norms, risk analysis, audit results, and related action.
- **Information Security Manager/Officer:** They advise top management on information security, aligning business and security objectives, identifying budgets, and drafting information security policies.
- **System and Information Owners:** Business owners in charge of processes and data define protection requirements and ensure information security controls are in place and effective

A thorough evaluation of the organisation's context is crucial when establishing information security requirements. This involves assessing the organisation's reliance on the internet and cloud services, the impact of regulations, and potential threats by consulting with information and asset owners.

Based on this evaluation, SMEs should design, apply, and monitor information security controls. Top management should evaluate actions needed to address risks, along with their timing and funding, and they should implement cost-efficient protective measures.

An information security plan should be created to identify and prioritise controls based on potential threats to physical assets, ensuring they are applied to relevant assets. Regular monitoring of these implemented controls for malware protection, vulnerability patching,

and incident response is also critical.

Furthermore, the organisation’s top management should acknowledge information security as a key enabler and actively promote and fund initiatives to reduce information security risks, ensure legal and contractual compliance, and adhere to sectoral good practices. All internal and external personnel are expected to follow the information security policy, with disciplinary actions possible for non-compliance.

2. Risk Management

To effectively undertake cybersecurity risk management, SMEs should establish a continuous cycle of planning, implementation, operation, and improvement, fostering a risk-aware culture.

Key steps in this process include:

1. Establishing a Risk Management Framework: Develop and maintain a structured approach to identifying, assessing, managing, and mitigating cybersecurity risks. A documented framework is useful for this purpose.

2. Identifying and Valuing Assets: Recognise and value all information and associated assets crucial to the organisation. Understanding the connections between these assets is crucial for determining the necessary information security protection.

3. Understanding the Context: Gain a deep understanding of the environment in which the organisation operates to define information security requirements effectively.

- Evaluate the organisation's reliance on the internet, cloud services, and the impact of relevant regulations and contractual obligations.
- Consult with information and asset owners to identify potential threats.
- Relate identified threats to established cybersecurity threat models, such as the ENISA model, to consider potential risk causes.

4. Designing, Applying, and Monitoring Security Controls: Determine which security controls to implement or improve. Top management should evaluate the actions needed to address each identified risk, including considerations for timing and funding. Selected protective measures should be both effective and cost-efficient.

- Establish an Information Security Plan to identify and implement necessary controls.
- Manage this plan to ensure its ongoing effectiveness.

5. Treating Risks: Develop risk treatment plans that align with regulatory guidelines and assign clear responsibilities for executing these plans. Entities can choose from four risk treatment options: avoidance, mitigation, transfer, or acceptance.

- **Avoidance**: if you deem the impact of an incident occurring too high to be accepted, you can choose to avoid the risk by ending the process or preventing the activity that would cause the risk. For example, if storing customer data in the cloud is deemed too high a security risk, you can avoid the risk by only storing data offline.
- **Mitigation**: risk mitigation can be achieved by installing and utilising security controls. For instance, to reduce the risk of malicious actors accessing payroll details, you can implement role-based access controls and cryptography to prevent data from falling into the hands of such individuals.
- **Transfer**: if avoiding a risk is not possible and mitigation techniques do not sufficiently protect against the impact of an event, you can transfer the impact through insurance. This does not transfer the full impact, as factors such as business reputation and client trust may still be impacted, but it will at least transfer the majority of the financial risk.
- **Acceptance**: if the impact or likelihood of a risk is deemed insignificant, you may choose to accept the risk by not applying any of the steps above.

6. Monitoring: Regularly monitor implemented controls, such as those for malware protection, vulnerability patching, and incident response, to ensure they are functioning as intended.

7. Independent Review: Ensure that an independent entity with the appropriate cybersecurity knowledge, industry understanding, risk assessment skills, and compliance knowledge conducts reviews.

8. Policies and Procedures: Establish and implement policies and procedures to effectively assess whether cybersecurity risk-management measures are properly implemented and maintained.

9. Review and Update: Regularly review risk assessments and treatment plans, incorporating change logs and comments to keep them current and effective.

3. Incident Management

Incident handling is another critical area. A coherent incident handling policy, aligned with business continuity and disaster recovery plans, should include a categorisation system for incidents and effective communication plans.

The categorisation system should identify the consequences and priority of incidents, using criteria such as impact on business operations, data sensitivity, and legal and regulatory impact. Incident handling should encompass system failures, malicious code, denial of service, errors, breaches of confidentiality, and misuse of systems.

Communication plans should detail the purpose, scope, roles, responsibilities, and reporting mechanisms, while events should be reported by employees, suppliers, and customers through a simple mechanism.

Events should be assessed to determine if they constitute incidents, based on predefined criteria, with recurring incidents assessed quarterly. Incident response should follow documented procedures, considering priorities and impact, and may involve forensic activities and operational IT objectives.

Post-incident reviews should identify root causes and document lessons learned, assessing the effectiveness of risk treatment measures.

Each of the steps can be explained in turn:

Step 1: Identification

- Monitor security alerts and reports for unusual activity.
- Employees must immediately report suspicious incidents to the IT/Security Lead.
- Confirm the incident through system logs, threat intelligence, or external reports.

Step 2: Containment

- **Short-term**: Isolate affected systems (e.g., disconnect compromised devices from the network).
- **Long-term**: Apply patches, update credentials, and strengthen security controls.

Step 3: Eradication

- Remove malicious software or unauthorised access.

- Identify and fix vulnerabilities that led to the incident.
- Conduct security scans to confirm threat removal.

Step 4: Recovery

- Restore systems and data from backups.
- Monitor systems for signs of reinfection or residual threats.
- Resume normal operations with enhanced security controls.

Step 5: Communication & Reporting

- **Internal**: Notify employees and relevant departments as needed.
- **External**: Inform affected customers, partners, or regulatory bodies (if required by law).
- **Law Enforcement**: Report major breaches (e.g., data theft, financial fraud) to authorities.

Step 6: Prevention & Continuous Improvement

- Regular cybersecurity awareness training for employees.
- Implement strong access controls and multi-factor authentication.
- Conduct periodic security audits and penetration testing.

Step 7: Lessons Learned

- Conduct a post-incident review to analyse root causes and response effectiveness.
- Update security policies, training, and controls based on findings.
- Document the incident and response actions for compliance and future reference.

4. Business Continuity

SMEs can ensure business continuity by developing and maintaining a business continuity and disaster recovery plan, focusing on backup management, and establishing a crisis management process.

A business continuity and disaster recovery plan should be in place to be applied in the case of incidents. The plan needs to be based on risk assessment results and include key elements. The plan should include:

- Purpose, scope, and audience
- Roles and responsibilities
- Key contacts and communication channels
- Conditions for plan activation and deactivation
- Order of recovery for operations
- Recovery plans for specific operations, including objectives
- Required resources, including backups and redundancies
- Restoring and resuming activities from temporary measures

To ensure the plan's effectiveness, SMEs should:

- Test, review, and update the business continuity and disaster recovery plans at planned intervals, especially after significant incidents or changes to operations or risks. These should occur at least annually.
- Incorporate lessons learned from tests into the plans.
- Keep logs of business continuity plan activation and execution.
- Determine the order of recovery based on asset classification, service importance, dependencies, recovery objectives, resource availability, and regulatory requirements.
- Conduct capacity planning for information processing, telecommunications, and environmental support after business continuity plan activation.
- Prepare for service recovery and restoration after a disaster, identifying measures like failover sites and remote backups.

- Make sure third-party services will be available in case of disaster (e.g. hot site).
- Communicate changes to related key personnel.
- Protect business continuity and disaster recovery plans from unauthorised disclosure and modification.

Business Impact Analysis (BIA): SMEs should conduct a BIA to assess the potential impact of severe disruptions to their business operations and establish continuity requirements for network and information systems based on the analysis results. Appropriate recovery objectives should also be established.

Backup management is another key component of ensuring business continuity. SMEs should maintain backup copies of data and provide sufficient resources to ensure an appropriate level of redundancy. Backup plans should include recovery times, assurance of complete and accurate backup copies, safe storage locations, appropriate physical and logical access controls, data restoration procedures, and retention periods based on business and regulatory requirements. Regular integrity checks on backup copies are essential. The frequency of backup checks should be tailored to the data criticality based on the risk assessment. Additionally, the redundancy of network and information systems, facilities, and personnel should be ensured.

SMEs should establish a **crisis management** process to ensure business continuity. The crisis management process should address roles and responsibilities, internal and external communications, and coordination with relevant parties. The communication element might describe how information will be disseminated to stakeholders during a crisis, templates for communication, and up-to-date contact information for internal and external stakeholders. The crisis management plan should be tested, reviewed, and updated regularly or following significant incidents or changes.

5. Supply Chain Security

In terms of supply chain security, SMEs should implement a **supply chain security** policy covering risk assessment, security requirements, supplier selection, contract clauses, monitoring, and incident management. A directory of suppliers and service providers should be maintained, including contact points and ICT services provided. ICT supply chain security requirements should be established, validated, and reviewed, focusing on detecting and protecting against unauthorised changes.

6. Network and Information System Security

To establish effective cybersecurity measures, small and medium-sized enterprises (SMEs) should focus on several key areas. It is essential to have a **policy on the security of network and information systems**, which should be updated based on changes in legislation, feedback, independent reviews, recommendations from authorities, violations, exceptions, and incidents. A documented policy should be maintained, ensuring it is confidential, integral, available, complete, correct, understandable, identifiable, and retrievable.

To ensure compliance, SMEs should **regularly review their adherence to network and information system security policies**, topic-specific policies, rules, and standards, reporting the status to management. An independent review of the approach to managing network and information systems is also crucial, with results reported to management and corrective actions taken.

7. Cyber Hygiene

Business continuity and disaster recovery plans are essential, based on risk assessments, and should include elements such as purpose, scope, roles, communication channels, activation conditions, recovery order, resource requirements, and restoration activities. These plans should be tested, reviewed, and updated regularly, incorporating lessons from tests and communicating changes to personnel. Backup management is crucial, with copies of data maintained and sufficient redundancy ensured. Crisis management processes should address roles, communications, and coordination, tested and updated regularly.

Configuration management is also vital, with documented baseline configurations and regular reviews. Change management procedures should control changes to network and information systems, with reports describing steps and results. Security patch management procedures should align with change and vulnerability management, with vulnerability assessments conducted regularly. Network security should be managed through rule sets for traffic filtering, intrusion detection, and prevention. Network segmentation should be based on risk assessments, separating systems and networks from third parties. Protection against malicious software should include detection, prevention, and removal measures, with documented alternative countermeasures.

Finally, **asset management** requires a complete, accurate, and up-to-date inventory of assets, with periodic reviews of classification levels. A policy for the proper handling of assets, including those used off-premises, should be in place. A removable media policy should technically prohibit connections unless there is an organisational reason, provide for disabling self-execution, and include measures for data protection. Procedures should ensure that assets are deposited, returned, or deleted upon termination of employment. Environmental and physical security should prevent loss or damage due to utility failures and physical threats, tested and updated regularly.

8. Human Resources Security

Human resources security involves ensuring that employees, direct suppliers, and service providers understand and commit to their security responsibilities. These responsibilities should align with their roles, the services they offer, and the company's network and information security policies.

Key aspects of human resources security include:

- **Defining roles, responsibilities, and authorities** for network and information system security and assigning them to specific roles.
- Ensuring that **management body members** understand and act in accordance with their responsibilities regarding network and information system security.
- Establishing **mechanisms for hiring qualified personnel**, such as reference checks, vetting procedures, validation of certifications, or written tests.
- **Regular awareness training** on cyber hygiene practices tailored to different roles.
- Applying **security training** to staff members who transfer to new positions or roles requiring security-relevant skill sets and expertise.
- **Verification of the background** of employees and direct suppliers, and service providers, where applicable.
- Contractually defining and enforcing **network and information system security responsibilities and duties** that remain valid after termination or change of employment.
- Establishing, communicating, and maintaining a **disciplinary process** for handling violations of network and information system security policies, considering legal, statutory, contractual, and business requirements.

Several elements can serve as evidence of human resources security

- Lists of employees and their assigned roles.
- Documented evidence of regular training sessions on network and information systems security for employees, direct suppliers, and service providers.
- Signed acknowledgements from employees, direct suppliers, and service providers confirming they have read, understood, and agreed to comply with the policy.
- Reports from internal or external audits assessing the understanding and implementation of security responsibilities.
- Inclusion of security responsibilities in employee performance reviews and evaluations.
- Contracts with direct suppliers and service providers that include clauses on security responsibilities and compliance with the entity's policies.

Human resources security also involves **screening personnel** and incorporating **contract clauses**. Criminal history and background checks should be conducted for employees and third-party personnel with regular access to the organisation's premises, in accordance with laws, regulations, and ethics. Non-disclosure agreements should be signed by all employees and third-party personnel before any interaction with the organisation's information, and their contracts should require adherence to the organisation's information security policies, with clearly defined consequences for violations, even after position changes or termination.

9. Access Control

To effectively manage access control, it is important to **establish, document, implement, and maintain both logical and physical access control policies** that align with your organisation's business and security needs. This begins with a comprehensive policy that encompasses access by personnel (staff, visitors, external entities) and network/ information system processes, ensuring that only adequately authenticated users are granted access. This policy should undergo regular reviews, at least annually, and be updated following significant incidents or changes.

Managing access rights involves providing, modifying, removing, and documenting these rights in accordance with the access control policy. This includes assigning and revoking access based on the **principles of need-to-know, least privilege, and separation of duties**, as well as modifying access rights upon termination or changes in employment. Access to network and information systems should be authorised by relevant personnel, with third-party access (visitors, suppliers, service providers) limited in scope and duration, and governed by signed agreements acknowledging responsibilities. Maintain a register of granted access rights, detailing user-names, roles, permissions, and dates of access changes, alongside logging the management of access rights, specifying who granted/modified access, when, and what changes were made. Regular reviews of physical and logical access rights should occur, considering users' access rights post-termination or changes in employment, and authorisations for privileged access rights. Access control reviews of assets should be performed at least annually to validate that all privileges are authorised, documenting the results and necessary changes to access rights.

Implementing access control rules requires defining and mapping appropriate access rights and restrictions to human users or system processes, with granularity determined by business requirements and risk assessment results. Consistency between access rights and asset classification, as well as physical perimeter security needs, should be considered, alongside all types of available connections in distributed environments and dynamic elements in access control rules. Access control can be implemented using methods such as MAC (mandatory access control), DAC (discretionary access control), RBAC (role-based access control), and ABAC (attribute-based access control), depending on business needs. Where supported, centralise access control for all assets through a directory service or SSO provider.

Policies for privileged accounts and system administration accounts should be maintained as part of the overall access control policy. Allocate privileged access rights based on competence and minimum role requirements, maintaining an authorisation process and record of all allocated privileged access rights. Establish strong identification,

authentication (such as multi-factor authentication), and authorisation procedures for privileged accounts. Set up specific accounts exclusively for system administration operations, individualising and restricting system administration privileges to the highest extent possible. System administration accounts should only connect to system administration systems, with defined expiry requirements for privileged access rights and temporary privileged access granted only for the necessary time. Log all privileged access for audit purposes and regularly review access rights of privileged accounts, documenting the results.

Restrict and control the use of system administration systems in accordance with the access control policy, ensuring they are used only for system administration purposes and logically separated from application software not used for system administration. Protect access to these systems through authentication and encryption, implementing strict access controls to ensure they are exclusively used for their intended purpose and physically or logically isolate them from other application servers through network segmentation.

Managing the lifecycle of identities of network and information systems and their users is crucial, including maintaining an inventory of all identities managed within the entity. Only permit identities assigned to multiple persons where necessary for business or operational reasons, subject to explicit approval and documentation.

Secure authentication procedures and technologies should be implemented based on access restrictions and the access control policy, including password-based authentication, multi-factor authentication (MFA), biometric authentication, token-based authentication, certificate-based authentication, and single sign-on (SSO). Ensure the strength of authentication is appropriate to the classification of the asset to be accessed and control the allocation and management of secret authentication information through a process ensuring confidentiality. Require changes to authentication credentials initially, at predefined intervals, and upon suspicion of compromise, using state-of-the-art authentication methods and unique authentication information. Authentication procedures and technologies should be reviewed regularly.

Multi-Factor Authentication (MFA) implementation should ensure the strength of authentication is appropriate for the classification of the asset being accessed. Determine which systems require MFA based on asset classification, and consider MFA when accessing systems remotely or at unusual times.

Communication and regular awareness raising on cyber hygiene practices should be implemented for all users, tailored to different roles and responsibilities.

10. Cryptography

To set up cryptography, companies should **establish, implement, and maintain a comprehensive policy and related procedures** to ensure data confidentiality, authenticity and integrity, following asset classification and risk assessment results.

The cryptography policy and procedures should define the types, strength, and quality of cryptographic measures required to protect assets, both data at rest and in transit, potentially adopting a cryptographic agility approach. This involves selecting approved protocols or families of protocols, cryptographic algorithms, cipher strength, cryptographic solutions, and usage practices.

Key management approaches should be defined, including methods for generating, issuing, obtaining, distributing, storing, archiving, and destroying keys. Cryptographic mechanisms like digital signatures and hashes should be used to protect the confidentiality and integrity of data in transit and at rest, to detect unauthorised changes to critical data, and to ensure secure data disposal after lawful use. Mechanisms (manual or automated) should be set up for selecting, establishing, managing and updating cryptographic keys.

Encryption should be used for sensitive information transfer, such as key generation and key management, and enforced on electronic media containing confidential or sensitive information. Data confidentiality and integrity should be ensured with cryptographic mechanisms when sharing information, scanning, using secure online and offline storage, and removing sensitive data from storage media.

Information availability should be maintained in case of lost cryptographic keys, like key escrowing. Symmetric and asymmetric cryptographic keys should be produced, controlled and distributed using key management technology and processes, with automated cryptographic key management mechanisms used to generate keys, obtain public key certificates, distribute keys to users, and deal with compromised keys. Logs should be kept for key management activities like key generation, destruction and archiving. Cryptographic keys should be protected against modification and loss, and secret and private keys should be protected against unauthorised use and disclosure. The authenticity of public keys should be ensured, and equipment used to generate, store and archive keys should be physically protected. The use of ad-hoc cryptographic processes should be limited.

To maintain an effective cryptography set-up, a company should ensure the cryptography policy aligns with industry standards and advancements and review the cryptography policy and procedures at least annually. A procedure should be maintained specifying how

cryptography policy and procedures are reviewed, including responsible personnel and review intervals. Changes to cryptographic measures should be tested before implementation, and these changes should be communicated to employees. Employees should be trained and made aware of the use of cryptographic measures. Network and information systems should automatically encrypt and secure all portable and removable media.

Chapter 5: Risk assessment and reporting: what does the NIS2 prescribe?

Risk Assessment Methodology

The implementation of the NIS2 Directive requires organisations, including SMEs, to establish strong risk management frameworks to ensure the security of their network and information systems. This framework should be designed to be comprehensive, continuously updated, and integrated into the organisation's overall risk management process.

At the heart of this process is the risk assessment methodology, which helps identify, analyse, evaluate, and manage risks. These risks may affect the availability, integrity, confidentiality, and authenticity of critical systems, particularly those involving third parties. To comply with the NIS2 Directive, SMEs must ensure that their management bodies are informed and proactively engaged in reviewing and approving residual risks.

The **Cooperation Group** plays an essential role in supporting and standardising the risk assessment process across the EU. It facilitates cooperation among Member States, the European Commission, and ENISA to strengthen trust and cybersecurity resilience. This means conducting coordinated security risk assessments of specific ICT supply chains focusing on critical services, systems, and products.

Key Components of a Risk Management Framework

Organisations are required to establish a structured approach to cybersecurity risk management. This includes:

1. Identifying Risks: SMEs must document potential risks to their network and information systems. This includes risks related to third party suppliers, external threats, and internal vulnerabilities. Particular attention should be paid to single points of failure that could disrupt operations.

2. Risk Analysis: this involves understanding the likelihood and potential impact of identified risks. Cyber threat intelligence and known vulnerabilities must be factored into this analysis to accurately measure the risk level.

3. Risk Evaluation: once risks are analysed, they should be evaluated against predefined criteria to determine their significance and prioritise mitigation efforts.

4. Risk Treatment: Organisations must develop a risk treatment plan that outlines measures to mitigate, transfer, accept, or avoid risks.

5. Monitoring and Review: risk assessments and treatment plans must be regularly updated to reflect changes in the operational environment, emerging threats or significant incidents.

The NIS2 Directive aims at strengthening the cyber resilience and the cyber hygiene baseline of SMEs and highlights supply chain security due to increasing reliance on third-party ICT services, systems, and products. SMEs must extend their risk assessments to evaluate the security posture of their suppliers and partners and they must document their chosen security measures and provide clear justifications for any residual risks. This documentation should be accessible and comprehensible to both technical teams and management. Moreover, key staff members within the organisation should be made aware of the primary risks and the steps being taken to mitigate them.

What are some practical steps for SMEs?

SMEs can take the following steps to simplify implementation:

1. Adopt standardised risk assessment tools such as the ISO/IEC 27001 framework. DIGITAL SME has written a guide on how SMEs can adapt this standard for their organisation.
2. Leverage DIGITAL SME Cyber guidelines, as there is tailored guidance for SMEs, particularly on supply chain management.
3. Engage in staff training so that employees understand their role in the cybersecurity risk management process. In a cybersecure organisation, the whole staff makes up the security team.

Staff Training

Staff training is an essential component for SMEs, especially when it comes to suppliers of NIS2-compliant entities. SMEs must ensure their employees are equipped with the knowledge and skills to comply with the cybersecurity requirements of their clients while also meeting their own compliance obligations.

Practical and targeted training programmes can make a significant difference in reducing risks and maintaining trust with larger partners.

How to Report

Essential and important entities across EU Member States are required to report incidents that significantly impact their services. A “significant incident” is one that either causes or risks causing major service disruption or financial loss, or impacts individual or other organisations, potentially causing notable damage.

What do the reporting process and timeline look like?

1. Initial Reporting: within 24 hours of becoming aware of a significant incident, the affected entity must send an Early Warning to the national CSIRT or to the relevant NIS2 authority. Make sure to check which entity is considered the NIS2 authority in your country. This notification should indicate whether the incident might be due to unlawful activities and if it has cross-border implications. Upon receiving an Early Warning, the CSIRT or competent authority should provide initial feedback within 24 hours, offering guidance on possible mitigation measures.

2. Comprehensive Incident Notification: within 72 hours of incident awareness, a more detailed incident notification must be provided, expanding on the initial information. This update should include an initial assessment of the incident's severity and impact, as well as any indicators of compromised networks.

3. Final Reporting: after the incident notification, additional updates may be required. Upon the NIS2 authority's request, an intermediate report could be provided with relevant status updates. A Final Report must be submitted no later than one month from the initial notification, detailing the overall impact of the incident, including:

    a. Root cause of the incident

    b. Severity of the incident

    c. Ongoing mitigation measures

If the incident is ongoing at the one-month mark, a Progress Report should be submitted with the latest developments, followed by a Final Report upon incident resolution.

Entities must inform potentially affected service recipients about the threat itself and any preventive or mitigating actions they can take. In cases where public awareness could help prevent harm or mitigate an ongoing incident, CSIRTs or the relevant authorities may, after consulting with the entity, decide to disclose details of the incident to the public or require the entity to do so.

Chapter 6: Interplay with other legislations

As cybersecurity regulations evolve across the EU, organisations must navigate an increasingly interconnected landscape of compliance requirements. For SMEs, three key regulations – NIS2, DORA and the CRA – have become central to ensuring security and resilience. Even if each regulation targets distinct sectors and objectives, they share overlapping principles and compliance areas that SMEs must address effectively.

Key Overlapping Areas

Risk Management

Risk management is a core requirement across all three regulations. While their focuses differ as NIS2 emphasises critical infrastructure, DORA targets operational risks in the financial sector, and CRA prioritises product security, they share foundational principles.

What can SMEs do to accommodate the requirements of these regulations?

NIS2, DORA and the CRA share several key overlapping areas which SMEs can address through an integrated approach to streamline compliance. All three regulations highlight effective risk management, requiring businesses to assess and mitigate cybersecurity risks across their operations, supply chains, and products. All three regulations encourage adherence to recognised standardisation and best practices such as adopting frameworks like ISO/IEC 27001 and secure-by-design principles, to strengthen resilience and compliance. By focusing on these common areas, SMEs can create a cohesive cybersecurity strategy that meets the requirements of all three regulations while increasing overall operational security.

Interplay with the CRA

The CRA (Cyber Resilience Act) will play a crucial role for the enhancement of cybersecurity in Europe. The EU Act is valid for products with digital elements, which by default applies to any product that contains software or even pure software products. The CRA applies, similar to other European Acts, a risk-based approach to evaluate whether a product has to comply with higher security measures than others. Most of the software is covered by the “consumer” side: around 80% of all (software-) products fall under this category. As soon as critical resources, i.e. services that fall under the NIS-2 directive, are impacted by the software, the CRA applies stricter rules. An exception to the rule above are pure OpenSource components that do not bear any sign of making a profit (pure hobbyist projects).

For other open source projects the model of stewardship will be applied: some entity has

to take the ownership of the component and plan and apply the rules of the CRA to the software.

There are technical and organizational measures that companies and organizations have to meet.

Disclaimer: Listed measures are subject to change and could be incomplete. Please always refer to the latest version of the CRA itself and consult with a professional.

The main organisational measures for CRA software include:

- Users must be able to report security vulnerabilities, and the provider of the CRA software has to report software vulnerabilities to the national coordination centre and to CVE databases within a certain amount of time. This enables customers to react promptly to possible critical exposures and eliminates the black market for vulnerabilities, where attackers can buy “unknown” CVE for software products. Fixes for vulnerabilities have to be provided as per the next rule.

- The maintenance and publication of security fixes for the period of five years for each release. The CRA mandates that these security fixes have to be applied cost-free for the users of the software. In consequence, companies especially have to take care that new features are not mixed with security fixes, because otherwise the new features will be offered for free as well. A stricter release management is the consequence, as well as a adoption of a different business model.

- To maintain a catalogue of used software libraries and the bill of materials (SBOM). Especially SBOM allows companies to search for vulnerabilities in an efficient way and will pave the path to an automated processing of vulnerabilities.

- If software companies use open-source software in their products, they have to take the accountability for this software as well, i.e. they have to apply bug fixes to the open source software as if it would be their own software. This guarantees that the vast ecosystem of open-source components also benefits from the rules of the CRA. If companies are unable to supply a fix, they have to take other measures or remove the open-source component from their product.

- The documentation of measures that have been applied in the software stack. The documentation must be made available and the EU will use the documentation to grant the CE mark for (software) products based on this documentation. As of this writing, it is unclear what exactly the documentation has to cover, and more details will be published in the coming years.

The main technical measures for CRA software include:

- The possibility to download security fixes for your software.
- The application of threat modelling for the (software) product. In the interconnected world of today there are many threats that have an impact on the operation of services. Threat modelling ensures that at least the most important threats are already covered and that new software products apply a bare minimum of the possible security defences. Threat modelling usually happens on the base of attack vectors of the user, the application, the network or the physical system.
- The integration and application of a Secure Software Development Lifecycle. As software is being built, the documentation for technical security measures should already be documented and applied. This not only eases the documentation of the software product, but it will ensure that authentication and authorization measures are applied early in the development. E.g. the application of „Security by Design and Default„ could ensure that default passwords have a minimum length of 12 characters and that they contain special characters. The application of “Fail Safe” ensures that systems fall back into a state where no additional damages can be expected.

The consequence for companies that offer services under the NIS-2 is that they should mainly use CRA compliant software in their stack. CRA compliant software is the supply chain for their services and they ensure that vulnerabilities in software stacks will be handled with needed attention. Of course, NIS-2 has to apply security fixes as soon as possible, based on their own risk profile. The CRA complements the security defences of NIS-2 service providers. If possible, NIS-2 companies should ask their software supply chain for CRA compliance starting now. Vendors have three years to apply the CRA rules to their software products until the rules become mandatory.

Conclusion

The NIS2 Directive establishes higher cybersecurity standards across the EU, impacting not only directly regulated entities but also their suppliers. As a supplier, understanding and aligning with NIS2 security expectations is essential to maintaining business relationships, ensuring trust, and demonstrating a commitment to cybersecurity.

This guide provides practical directions on how suppliers can meet the expectations of NIS2-compliant entities. By implementing risk management frameworks, security controls, and incident response measures, suppliers can proactively address cybersecurity risks and align with industry best practices. However, NIS2 compliance is ultimately the responsibility of regulated entities. Suppliers are encouraged to use this guide as a reference point to strengthen their security posture, better their market competitiveness, and support their client's compliance efforts.

Cybersecurity is an evolving challenge, and suppliers should continuously monitor regulatory developments, update security measures, and collaborate with their clients to establish a resilient supply chain.