wallix Steptoe

NIS 2 Directive Unpacked

All you need to know about the NIS 2 Directive

NIS 2 Directive Unpacked

All you need to know about the NIS 2 Directive

In the dynamic landscape of the digital realm, cyber threats are advancing exponentially, both in scale and complexity. As organisations globally embrace digital transformation, including the integration of artificial intelligence, the protection of sensitive data and critical infrastructure has become paramount.

As an enabler of a sustainable digital approach or a vehicle for the adoption of innovation and technology, cybersecurity which often appears as a constraint as long as standards aren't clear for every organisation, are digital "hygiene rules" about to emerge?

The Network and Information Systems Directive (NIS 2) plays a pivotal role in establishing a comprehensive framework to tackle the evolving challenges posed by cybersecurity. Positioned as a crucial component of the EU's cybersecurity strategy, the NIS 2 Directive aims to bolster the resilience of critical infrastructure and digital services. It builds upon its predecessor, the NIS Directive, by expanding its scope and imposing new obligations on a wider array of entities, including digital service providers.

Effectively navigating the intricate legal landscape of the NIS 2 Directive necessitates a nuanced understanding of both legal and technical aspects, demanding a holistic approach to cybersecurity. Additionally, collaborative efforts across disciplines and expertise are essential for the successful implementation of the NIS 2 requirements.

To bridge this gap, Steptoe and WALLIX have synergized their respective regulatory and technical expertise, presenting a comprehensive guide on achieving compliance with the NIS 2 Directive.

Our White Paper not only translates legal requirements into tangible technical action points but also provides a roadmap with practical steps, empowering organisations in their compliance endeavors and their governance process to level up their cybersecurity.

Steptoe

wallix

NIS 2 Directive Unpacked

All you need to know about the NIS 2 Directive

Contents

Steptoe

wallix

Edito

Since its introduction in 2016, the Network and Information Systems Directive ("NIS Directive") has been the first significant milestone in European cybersecurity regulation. It has raised awareness of digital threats, established minimum security standards, and encouraged cooperation among European Union's (EU) Member States. However, in the face of ever-evolving cyber threats and technologies, it is imperative to acknowledge that substantial adjustments are needed. Cyber threats are continuously evolving, and regulations must evolve accordingly to protect critical infrastructures and uphold European digital sovereignty.

The assessment of the NIS Directive revealed shortcomings. Despite its significance, uneven enforcement and relatively lenient penalties have hindered its effectiveness. Financial penalties, often modest, have failed to incentivize companies to make substantial investments in their cybersecurity. The lack of deterrence has created an environment of insecurity.

In recent years, there has been a disconcerting surge in cybercrime, leaving both businesses and local communities grappling with severe consequences. The impact of these cyber threats has transcended mere financial losses, infiltrating the very fabric of our interconnected society. As the stakes continue to rise, there is an urgent call to fortify European IT infrastructure with resilience measures to safeguard against the escalating cyber onslaught.

Cybercriminals exploit vulnerabilities in IT systems, capitalizing on the increasing reliance on technology across sectors. Reports of ransomware attacks, data breaches, and identity theft have become alarmingly frequent, leaving a trail of financial ruin and compromised sensitive information.

Cybercrime is not confined to the corporate realm; local communities are equally vulnerable. Municipalities, government agencies, and public services have experienced a surge in attacks that disrupt essential services. From critical infrastructure to public safety systems, the impact of cyber incidents on local communities is far-reaching, eroding the very foundation of societal well-being.

In the face of this escalating threat landscape, the importance of building resilience in IT infrastructure cannot be overstated. Collaboration and concerted efforts are required to establish a united front against cyber threats.

As businesses and local communities grapple with the fallout, the need for a resilient IT infrastructure has never been clearer. By fostering collaboration, harmonizing regulations, investing in technology, and prioritizing education, the EU can build a robust defense against the escalating tide of cyber threats. The time to act is now to secure a digitally connected future for all.

The NIS 2 Directive in a nutshell

The NIS 2 Directive, which updates the 2016 NIS Directive, aims at modernizing the EU cybersecurity legal framework, taking into account the increased digitization of the internal market and the evolving cybersecurity threat landscape. To this end, it imposes stricter standards to bolster EU cyber resilience and digital sovereignty.

Extension of scope

Firstly, the NIS 2 Directive broadens the scope of the NIS Directive to include new strategic sectors, such as healthcare, transportation, and energy, acknowledging that cybersecurity is ubiquitous across all domains. It further introduces a pivotal shift from the previous distinction between "operators of essential services" (OES) and "digital service providers" (DSP) to a more nuanced categorization of entities as "essential" or "important." This categorization is automatic and is primarily based on entity size and sector involvement.

Detailed cybersecurity specifications

The NIS 2 Directive imposes more detailed specifications of cybersecurity measures, stringent rules governing incident reporting, and enhanced and more specific sanction regime. Notably, responsibility is explicitly assigned to senior management within each entity, elevating cybersecurity to a pivotal boardroom concern.

Enhanced cyber-resilience cooperation

The NIS 2 Directive further mandates increased collaboration among European stakeholders, fostering more robust cooperation mechanisms to address cross-border threats. National governments, including the various national Computer Security Incident Response Teams (CSIRTs), are mandated to augment their influence and foster increased collaboration. National cybersecurity strategies must evolve, incorporating crucial elements such as active cyber protection and tailored policies catering to the unique challenges faced by Small and Medium Enterprises ("SMEs"). This necessitates the establishment of coordinated vulnerability disclosure frameworks and dedicated cybersecurity crisis management authorities, as outlined in the NIS 2 Directive. European cooperation is expanding on multiple fronts. At the policy level, the NIS Cooperation Group facilitates collaboration, while the EU CSIRTs network enhances technical collaboration. Crisis management efforts are streamlined through the establishment of the Cyber Crisis Liaison Organisation Network (CyCLONe). Regular Peer Reviews for Member States, biennial publication of a Cybersecurity State of the Union by the European Union Agency for Cybersecurity ENISA, and the creation of a European vulnerability database further solidify the collaborative framework. The NIS 2 Directive reinforces the need for sharing incident information and coordinating actions for a more effective response. It also acknowledges the central role of national and local authorities in safeguarding critical infrastructures.

National cybersecurity strategy

Each EU Member State must adopt a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity.

Enforcement

The NIS 2 Directive introduces more stringent enforcement regime and sanctions, which are differentiated between "essential" and "important" entities.

EU Member States must transpose the NIS 2 Directive into their national legal framework by 17 October 2024. **The obligations provided by the NIS 2 Directive will be applicable as from 18 October 2024.**

Who does the NIS 2 Directive apply to?

It applies to entities that are considered critical for the European Economic Area's (EEA) economy and society, the so-called "Essential Entities" and "Important Entities".

Important Entities vs Essential Entities

The classification depends on whether the entity falls under (i) a very critical or a critical sector, (ii) the size, and (iii) revenue of that entity.

Entity	Employees	Revenue	Sectors	
			Very Critical	Critical
Large entity	n ≥ 250	▪ Annual turnover ≥ €50M • Balance sheet total: z ≥ €43M	Essential	Important
Medium entity	250 ≥ n ≥ 50	€50M ≥ r ≥ €10M	Important	Important

⚠ **Some exceptions: There are certain types of entities that are classified as essential irrespective** of their size, such as:

- **Trust service providers;**
- **Top-level domain name;**
- **Domain name registration service providers; and**
- **Medium-sized entities that provide public communications networks and services.**

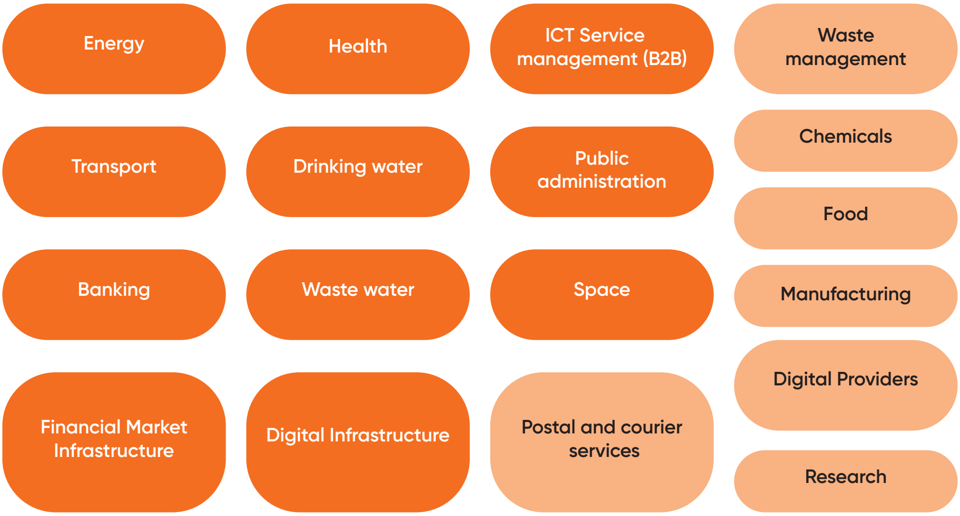
? What about small and micro entities?

In principle, small and micro entities, i.e. those with ≤ 50 employees and an annual turnover of less than €7 million (or a balance sheet total of less than €5 million), **do not fall within the scope of the NIS 2 Directive. However, EU Member States can decide to require small and micro entities to comply with the NIS 2 Directive obligations if they play a key role for the society, economy or for particular sectors or types of service.**

Critical Sectors vs Very Critical Sectors

The NIS 2 Directive affects more sectors than its predecessor, the NIS Directive. Precisely, the NIS Directive only designated the **types of entities that could potentially be considered as essential**, and only in the fields of Energy, Transport, Banking, Financial Market Infrastructure, Health sector, Drinking water supply and distribution, Digital infrastructure and Digital Service Providers; whereas it was left to **the Member States to identify which entities were ultimately considered as essential.** In contrast, the NIS 2 Directive provides for uniform rules which apply to **all large and medium-sized entities** providing their services or carrying out their activities within the EEA and in the **very critical and critical sectors.**

■ Very Critical □ Critical

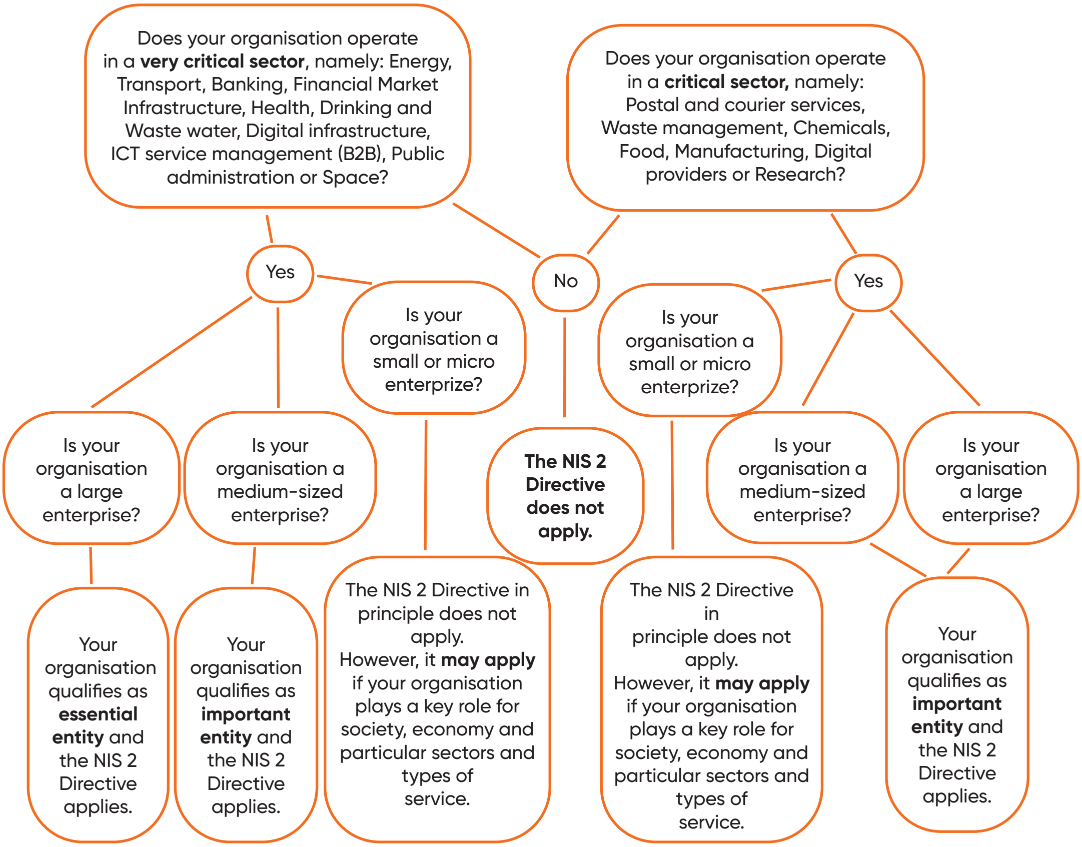


- ■ Energy
- ■ Transport
- ■ Banking
- ■ Financial Market Infrastructure
- ■ Health
- ■ Drinking water
- ■ Waste water
- ■ Digital Infrastructure
- ■ ICT Service management (B2B)
- ■ Public administration
- ■ Space
- □ Postal and courier services
- □ Waste management
- □ Chemicals
- □ Food
- □ Manufacturing
- □ Digital Providers
- □ Research

The NIS 2 Directive provides a detailed list of the types of entities operating in the sectors listed therein which fall in its scope. These types of entities are further defined in other EU and/or national laws, which have to be consulted before determining whether an entity falls within the scope of the NIS 2 Directive.

⚠ EU Member States have **until 17 April 2025** to establish their list of essential and important entities, as well as entities providing domain name registration services.

Will the NIS 2 Directive apply to your organisation?



Does your organisation operate in a **very critical sector**, namely: Energy, Transport, Banking, Financial Market Infrastructure, Health, Drinking and Waste water, Digital infrastructure, ICT service management (B2B), Public administration or Space?

Does your organisation operate in a **critical sector,** namely: Postal and courier services, Waste management, Chemicals, Food, Manufacturing, Digital providers or Research?

Yes

No

Yes

Is your organisation a large enterprize?

Is your organisation a medium-sized enterprise?

Is your organisation a small or micro enterprize?

The NIS 2 Directive does not apply.

Is your organisation a small or micro enterprize?

Is your organisation a medium-sized enterprise?

Is your organisation a large enterprize?

Your organisation qualifies as **essential entity** and the NIS 2 Directive applies.

Your organisation qualifies as **important entity** and the NIS 2 Directive applies.

The NIS 2 Directive in principle does not apply. However, it **may apply** if your organisation plays a key role for society, economy and particular sectors and types of service.

The NIS 2 Directive in principle does not apply. However, it **may apply** if your organisation plays a key role for society, economy and particular sectors and types of service.

Your organisation qualifies as **important entity** and the NIS 2 Directive applies.

** Certain exceptions apply, for example there are entities such as trust service providers, top-level domain name and domain name registration service providers, which are classified as essential irrespective of their size. Also, medium-sized entities that provide public communications networks and services, are considered as essential entities.*

Which obligations do organisations subject to the NIS 2 Directive need to comply with?

Cybersecurity risk-management measures

Supply chain risk assessment

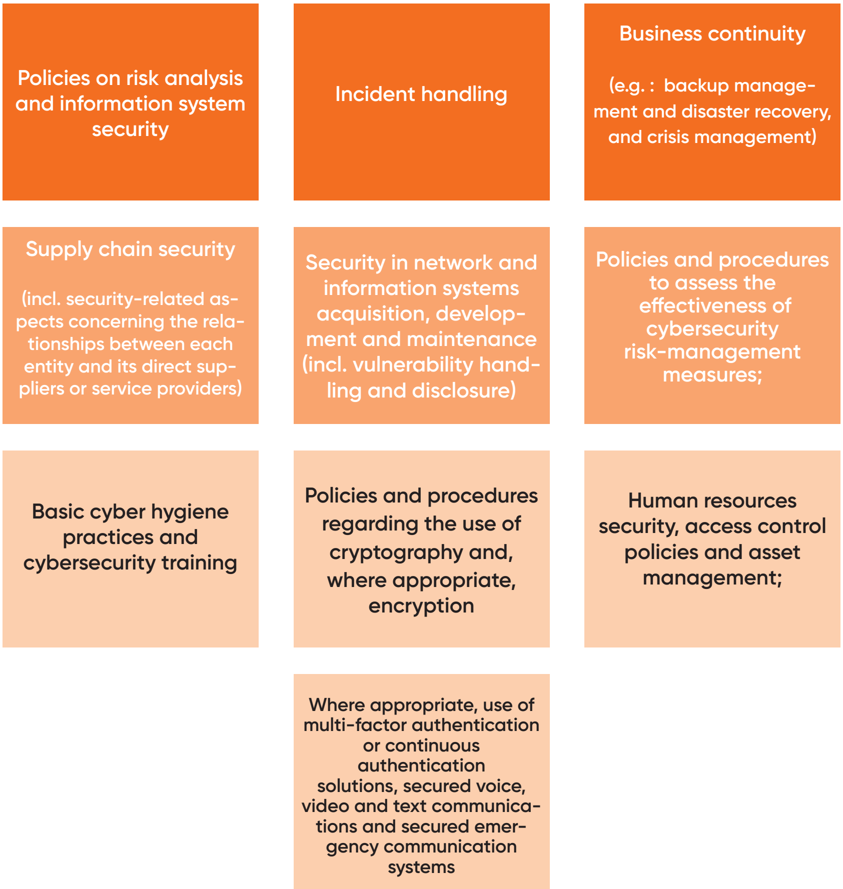
Governance

Incident reporting

Representative

Cybersecurity risk-management measures

- **Obligation for Essential and Important Entities to take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information** used for operations or for the provision of services, **and to prevent or minimize the impact of incidents** on recipients of their services and on other services, which must be based on an all-hazards approach and must include at least:



Policies on risk analysis and information system security

Incident handling

Business continuity

(e.g. : backup management and disaster recovery, and crisis management)

Supply chain security

(incl. security-related aspects concerning the relationships between each entity and its direct suppliers or service providers)

Security in network and information systems acquisition, development and maintenance (incl. vulnerability handling and disclosure)

Policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

Basic cyber hygiene practices and cybersecurity training

Policies and procedures regarding the use of cryptography and, where appropriate, encryption

Human resources security, access control policies and asset management;

Where appropriate, use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems

When assessing the proportionality of those measures, due account should be taken for:

- The degree of the entity’s exposure to risks;
- The entity’s size;
- The likelihood of occurrence of incidents; and
- The severity of incident, including their societal and economic impact.

⚠ **Please note that the use of particular ICT products, ICT services and ICT processes that are certified under European Cybersecurity Certification Schemes** may be required to demonstrate compliance with this obligation.

✓ Monitor guidelines and implementing acts to be issued by the European Commission regarding compliance with this obligation.

Supply chain risk assessment

- **Obligation for Essential and Important Entities to assess the vulnerabilities specific to each direct supplier and service provider, as well their overall quality of products and cybersecurity practices (including their secure development procedures**). To conduct such assessments, Essential and Important Entities are required to take into account the results of any coordinated security risk assessments of critical supply chains that may be carried out by competent authorities.

Governance

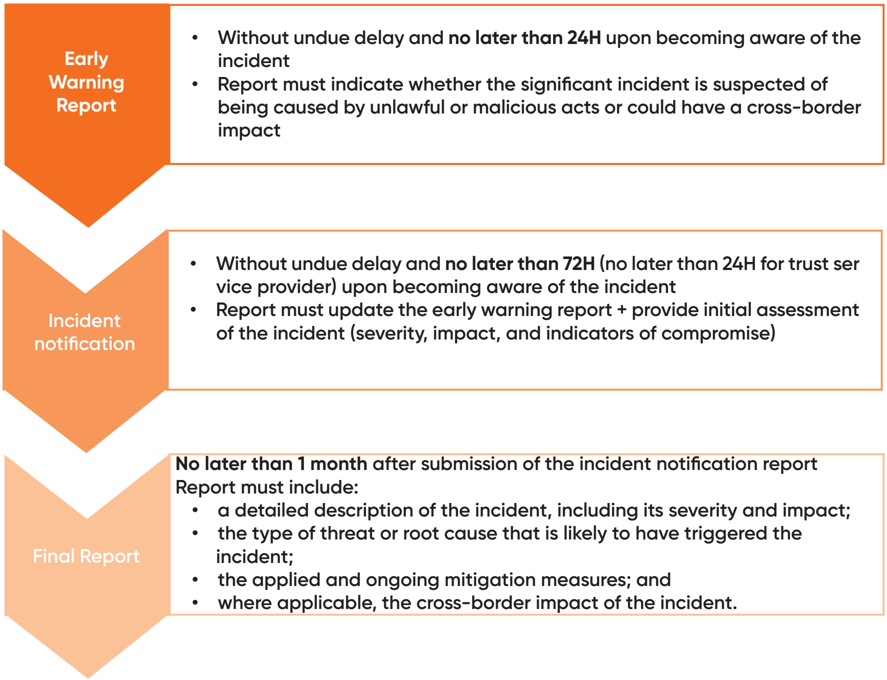
- **Obligation for management of Essential and Important Entities to:**

  - **Approve cybersecurity risk-management measures and oversee the implementation of such measures;**
  - **Follow training** on a regular basis to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by their entity;
  - **Ensure that their employees also have access to such training.**

⚠ Liability of management of Essential and Important entities in case of non-compliance with the obligation to adopt cybersecurity risk-management measures.

Incident reporting

- Obligation for Essential and Important Entities to notify competent national authority(ies) of any incident that has a significant impact on the provision of the services, in a three-stage approach*:



Early Warning Report

- Without undue delay and **no later than 24H** upon becoming aware of the incident
- Report must indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact

Incident notification

- Without undue delay and **no later than 72H** (no later than 24H for trust ser vice provider) upon becoming aware of the incident
- Report must update the early warning report + provide initial assessment of the incident (severity, impact, and indicators of compromise)

Final Report

No later than 1 month after submission of the incident notification report

Report must include:

- a detailed description of the incident, including its severity and impact;
- the type of threat or root cause that is likely to have triggered the incident;
- the applied and ongoing mitigation measures; and
- where applicable, the cross-border impact of the incident.

** Additional status update reports may be requested by competent national authority(ies)*

- Obligation for Essential and Important Entities to notify affected recipients of the services, without undue delay, of significant incidents that are likely to adversely affect the provision of those services.

- **Obligation for Essential and Important Entities to communicate to recipients of the services that are potentially affected by a significant cyber threat, without undue delay, any measures or remedies that they can take in response to that cyber threat and where appropriate, inform those recipients of the significant cyber threat itself.**

Representative

- **Obligation for Digital infrastructure providers and ICT service management (B2B) providers,** which are not established in the EU but offer services with the EU, **to designate a representative established in the EU.**

How compliance will be monitored, and which monetary sanctions can be imposed in case of non-compliance with the NIS 2 Directive?

Important Entities

- **Reactive supervision:** National competent authorities will take *ex post* enforcement actions when there is evidence and/or indication or information of non-compliance with the NIS 2 Directive.

- **Fines up to €7 million or 1.4% of the worldwide annual turnover.**

Essential Entities

- **Proactive supervision:** National competent authorities will actively monitor compliance with the NIS 2 Directive.

- **Fines up to €10 million or 2% of the worldwide annual turnover.**

How to prepare for compliance with the NIS 2 Directive?

Given the wide scope of obligations imposed by the NIS 2 Directive, Entities should not adopt a wait-and-see approach. Instead, they should already become **proactively prepared**. Such preparation notably entails assembling a **cross-department team** in order to ensure that **legal requirements are being translated into operational measures**. Wallix and Steptoe joined force to prepare a list of recommendations that will guide organisations on the compliance preparation steps that need to be taken from (i) a legal perspective and (ii) operational perspective.

Compliance Preparation Recommendations from a Legal perspective

✓ Assess the likelihood for your organisation or its customer(s) to fall within the scope of the NIS 2 Directive

Organisations active in the sectors listed as critical and/or very critical should already conduct an assessment on whether they are likely to fall within the scope of the Directive and if so, whether they will likely be qualified as "Essential" or "Important" entity.

Assessing whether customers are likely to fall within the scope of the NIS 2 Directive is equally important. Indeed, such customers will need to flow down their cybersecurity requirements on your organisation in order to comply with their supply chain risk assessment obligation under the NIS 2 Directive.

Please note however that the final determination of entities falling within the scope will be subject to the transposition of the NIS 2 Directive into EU Member States' national laws.

✓ Identify the jurisdiction(s) that you fall under and the national law(s) transposing the NIS 2 Directive that you will need to comply with

Since it is a Directive and thus not directly applicable, each EU Member State will need to transpose into its national law the obligations laid down in the NIS 2 Directive. Such national laws may foresee more stringent cybersecurity obligations than those provided by the NIS 2 Directive as the latter provides EU Member State with a margin of discretion regarding certain aspects. It is therefore of utmost importance for organisations to understand which national law(s) need(s) to be complied with.

Entities which are established in the EU will need to comply with the national law(s) transposing the NIS 2 Directive of all EU Member State(s) where they have an establishment. In practice, this means that if an entity has several establishments across the EU, it will need to comply with multiple national laws transposing the NIS 2 Directive.

⚠ Nonetheless, the NIS 2 Directive provides with some **exceptions**:

- **Providers of public electronic communications networks** or **providers of publicly available electronic communications services** will fall under **the jurisdiction of the Member State in which they provide their services** irrespective of whether or not they have an establishment in the Member State;
- **DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms,** which shall be considered to fall under **the jurisdiction of the Member State in which they have their**

main establishment in the Union, namely by elimination (i) the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken, (ii) the Member State where cybersecurity operations are carried out, or (iii) the Member State where the entity has the establishment with the highest number of employees in the Union.

- **Public administration** entities which will fall under **the jurisdiction of the Member State which established them.**

Entities which are not established in the EU but offer their services within the Union will fall under **the jurisdiction of the Member State where their representative is established**. Please note that in case of failure to designate an EU representative, any EU Member State in which the entity provides its services may take legal actions against this entity for infringement of the NIS 2 Directive.

✓ Provide information to competent authority(ies)

EU Member States must establish their list of Essential and Important Entities as well as entities providing domain name registration services **by 17 April 2025**. For the purpose of establishing this list, EU Member States will require the entities which meet the criteria of essential or important entities to provide:

- The name of their entity;
- The address and up-to-date contact details, including email addresses, IP ranges and telephone numbers;
- Where applicable, the sector and subsector in which they operate; and
- Where applicable, a list of the EU Member States where they provide relevant services.

It is thus important to monitor any call from competent authorities to **provide such information in the relevant jurisdiction(s) for your organisations.**

✓ Map your obligations, including any overlap with sectoral regulations.

In order to efficiently prepare the compliance programme, organisations must:

- Prepare a thorough and exhaustive list of obligations that will apply to them, taking into account not only the obligations provided by the NIS 2 Directive but also the national transposition in jurisdiction(s) relevant for them;
- Identify and document any overlap identified between the NIS 2 Directive and the sectoral legislations in regards to cybersecurity obligations;
- Conduct and document the gap analysis performed between what is currently in place and what is missing;
- Monitor the publication of national cybersecurity strategy and national regulators' guidelines in relevant jurisdictions, as well as European Commission's and ENISA's implementing acts, guidelines and templates.

✓ Review contractual arrangements with your supply chain

Organisations which fall within the scope of the NIS 2 Directive or whose customers fall within the scope of this Directive should already start identifying:

- The existing supplier/vendor/customer agreements that are to be reviewed in light of the requirements of the NIS 2 Directive;

- The process(es) and templates that will need to be updated to incorporate appropriate cybersecurity risk-management assessment and measures to ensure that appropriate protections are in place for future engagements.

✓ Budget for the time, human and financial investments required to comply

Compliance with the NIS 2 Directive will require significant human and financial investments. It is thus important that organisations start preparing by analysing notably:

- Whether they possess the required human resources to undertake this compliance effort;
- Whether they possess the required operational resources to undertake this compliance effort;
- How these will impact their upcoming budget needs and allocations.

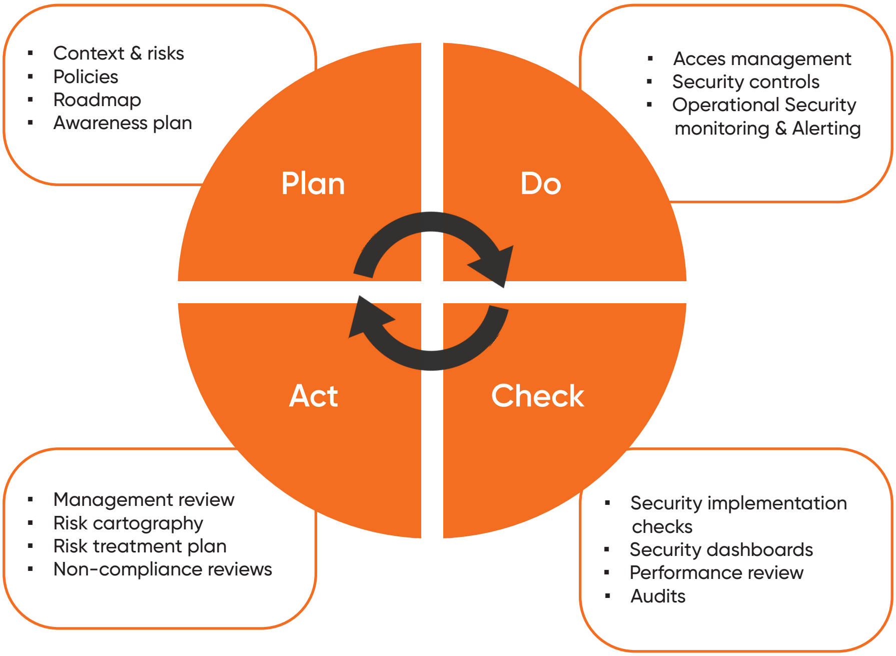
✓ For Digital infrastructure providers and ICT service management (B2B) providers established outside of the EU, appoint a representative

Digital infrastructure providers and ICT service management (B2B) providers that are established outside of the EU are required to appoint a representative established within the EU. The representative must be established in one of the EU Member States where the services are offered.

Compliance Preparation Recommendations from an Operational perspective

The forthcoming technical requirements under NIS 2 Directive are expected to seamlessly align with existing mandates set by national regulators. This continuity ensures a consistent cybersecurity framework, offering a foundation upon which entities can build and refine their systems.

The foundation of these measures lies in adopting a comprehensive all-hazards approach. This approach is designed to safeguard network and information systems, as well as the physical environment in which these systems operate, from various types of incidents. The NIS 2 Directive explicitly designates ISO27001 framework as a basis for security management.



- Context & risks
- Policies
- Roadmap
- Awareness plan

- Acces management
- Security controls
- Operational Security monitoring & Alerting

- Management review
- Risk cartography
- Risk treatment plan
- Non-compliance reviews

- Security implementation checks
- Security dashboards
- Performance review
- Audits

✓ Plan : Where do you need to go?

Effective cybersecurity begins with a thorough risk analysis according to the entity's business and regulations. Assessing the impact of significant scenarios, entities must develop information systems security policies that are aligned and proportionate with the risks and regulations that have a significant impact for them. This proactive approach, based on risk and integrating compliance is the cornerstone that must drive security implementation.

✓ Do: Pragmatic security implementation

Basic Cyber Hygiene Practices

Basic cyber hygiene practices form the foundation of a secure digital environment are a must-have. Most regulators already published some guidance on basic resilience. The assessment of implemented security mechanisms regarding these referential is definitely a good way to know where you are.

Regarding the NIS 2 Directive, regulators have not published yet technical security requirements. Nevertheless, we can reasonably assume they won't contradict themselves.

Prepare for Incident Handling

The question is not an organisation is going to be attacked but rapid and efficient incident handling is crucial in minimizing the impact of cybersecurity events. Establishing robust protocols for detecting, reporting, and responding to incidents ensures a swift and coordinated approach in mitigating potential risks. Good standards are published to help you drive incident resolution. Once again, the risk approach is a good starting point:

- What are the scenarios that can place your organisation under pressure?
- Who needs to be involved to solve the issue?
- Does your organisation have the skills and knowledge to remediate in an acceptable delay?
- Does your organisation need to reinforce its teams with external resources and consider a security incident response team (CSIRT)?
- Is your organisation properly insured?

Business Continuity, Backup Management, Disaster Recovery, and Crisis Management

Ensuring business continuity involves multiple elements:

- Clear understanding of the information and processing resources the organisation needs to operate;
- Meticulous backup management and periodic testing to ensure that backups are valid but also to ascertain the time needed for restoration;
- Sufficient backup externalization to cover any physical damaged of the organisation's IT facilities;
- A disaster recovery plan organizing the multiple operations required to restore a normal situation.

Prepare for a large security issues

Incident response and continuity procedures can be rightly designed, but still fall short in practice. Indeed, the technical capabilities are highly dependent upon the human intervention deploying them. It is therefore important to regularly test the effectiveness. of the incident and continuity procedures, and notably check:

- Whether your organisation is able to mobilize multiple ressources in a short period of time;
- Whether all information required to implement the procedures is available;
- Whether the necessary documentation and tools are accessible in a crisis scenario.

By enforcing and testing crisis management procedures, entities can navigate unforeseen disruptions, minimizing downtime and safeguarding the integrity of services provided.

✓ Check: Supply Chain Security

Organisations are rarely operating in an isolated fashion.. As with internal security, the security of the supply chain is a critical link in the cybersecurity chain. With the contract and the audit as a cornerstone, organisations must address security aspects related to their relationships with suppliers and service providers throughout the entire lifecycle – from acquisition and development to maintenance and termination. This includes robust security assurances and established contact points required to address the multiple security challenges.

✓ Act: Human Resource Security, Access Control Policies, and Asset Management

Human resource security, access control policies, and asset management are integral elements in protecting networks and information systems. Ensuring that personnel adhere to security protocols, implementing robust access controls, and managing assets effectively contribute significantly to overall cybersecurity resilience.
We often hear that humans are the weakest link in cybersecurity. We are

convinced that they are also the ultimate protection against an attacker! Therefore, building a robust awareness program for personnel is critical to ensure that they play an instrumental role in protecting the business.

✓ Check: Put security performance on the radar

Policies and Procedures Effectiveness Assessment

Continuous improvement is key to effective cybersecurity risk management. But to implement continuous improvement, security requires indicators for monitoring. Establishing dashboarding helps to assess the effectiveness of controls facing emerging threats risks and challenges.

Implement internal audit

Because trust does not exclude control, you need to implement periodical control of your teams and suppliers. If the correct execution of the procedures is not checked from time to time, it is highly likely that incorrect implementation would be unnoticed and that the security level expected would not be reached.

In that respect, it is important to stress that a wrongful implementation by a supplier can potentially have the same detrimental impact than an internal wrongdoing. Critical suppliers must be monitored similarly to internal resources to ensure the contract is fully applied.

✓ Act: Adapt your security posture

Adapt your posture to coming regulations

In the current context, the regulatory landscape is evolving fastly. It is thus important to frequently assess whether the security strategy remains aligned with the regulatory requirements. Due to the potential impact of a non-compliance and the increase of expectations of customers, compliance is more than ever a critical part of the business value.

Stay focused on your business risks

Some businesses are emerging while others are decreasing. Adapting your security strategy to business fluctuations is critical in controlling and adapting costs while always being concentrated on the valuable business which drives your company's future.

Conclusion

As we conclude this White Paper on the NIS 2 Directive, it is evident that this Directive represents a significant advancement in strengthening cybersecurity and digital sovereignty across the EU. Throughout our exploration of the NIS 2 Directive, we have emphasised its importance in addressing evolving cyber threats, fostering collaboration among stakeholders, and reinforcing the protection of critical infrastructures. Wrapping up our analysis, we wish to underscore two pivotal aspects, namely the effective management of the supply chain and the imperative need for European cybersecurity certifications

The management of the supply chain is increasingly recognized as a vital component of any cybersecurity strategy. With organisations relying on interconnected networks and third-party vendors, vulnerabilities within the supply chain pose significant risks. The NIS 2 Directive reflects this reality by emphasizing the necessity for organisations to assess and mitigate cybersecurity risks across their supply chains. By implementing robust supply chain security measures, organisations will bolster their resilience against cyber threats originating from external sources.

Furthermore, the establishment of European certifications - such as the European Cybersecurity Certification (EUCC) and the European Union Cybersecurity Scheme (EUCS) – plays a crucial role in fostering trust and harmonizing cybersecurity practices across the EU. These certifications will offer a standardized framework for evaluating and validating the cybersecurity capabilities of products, services, and processes. By encouraging the adoption of EU-certified solutions, the NIS 2 Directive aims to enhance the overall cybersecurity approach of organisations and contribute to the establishment of a more secure digital ecosystem.

It is essential to recognize that the NIS 2 Directive does not represent a deviation from existing security norms, standards, and best practices but rather an enhancement of them. As a matter of example, the NIS 2 Directive builds upon established frameworks, such as the ISO/IEC 27001 standard for information security management systems. By leveraging internationally recognized standards, the NIS 2 Directive ensures compatibility with existing cybersecurity practices while providing a cohesive framework for addressing emerging threats and challenges.

Looking ahead, the successful implementation of the NIS 2 Directive necessitates a collective effort from all stakeholders within the organisation, including Chief Security Officers, Chief Information Officers, C-suite, Legal, and more generally all personnel. Collaboration, information sharing, and continuous improvement will be pivotal in navigating the complexities of today's digital landscape and safeguarding critical infrastructures against cyber threats.

By embracing the principles of the NIS 2 Directive, we can forge a more resilient and secure digital future for our continent, grounded in trust, cooperation, and innovation.

STEPTOE

Steptoe is an international law firm focused on complex regulatory issues and litigation, with over 500 lawyers and other professionals in offices in Beijing, Brussels, Chicago, Hong Kong, Houston, London, Los Angeles, New York, San Francisco, and Washington. In more than 100 years of practice, Steptoe has earned an international reputation for effective representation of clients before public authorities, successful advocacy in litigation and arbitration, and creative and practical advice in structuring business transactions and advising on complex regulatory compliance.

Anne-Gabrielle Haie
aghaie@steptoe.com

Steptoe

WWW.STEPTOE.COM

For more information about Steptoe, the partners and their qualifications, see www.steptoe.com. These materials are not intended to constitute advertising, solicitation or legal advice, and you should not act (or refrain from acting) based upon these materials without obtaining professional advice regarding your particular facts and circumstances.

WALLIX

A European cybersecurity software company, WALLIX is a world leader in the identity and access management. With a strategy based on innovation and agility, WALLIX's mission is to simplify cybersecurity for its customers worldwide. The WALLIX suite of solutions is distributed by a network of more than 300 resellers and integrators worldwide and WALLIX supports nearly 3,000 organisations in more than 90 countries in securing their digital transformation. The company has been listed on Euronext (ALLIX) since 2015.

Jean-Noël de Galzain
jndegalzain@wallix.com

wallix

WWW.WALLIX.COM