EVIDEN
an atos business

Network and Information System Directive (NIS2) – Compliance Journey

Whitepaper

Eviden 2024

Authors:

Slawomir Pijanowski, Raducu Grigoras, Patricia Castro, Himanshu Mehta.

Contributors:

Kinga Michalak, Haroon Malik, Amir Salkic, Fabricio Lantieri, Paul Visser

Legal notice:

This publication represents the views and interpretations of EVIDEN unless stated otherwise.

EVIDEN has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only.

All references to it or its use as a whole or partially must contain EVIDEN as its source. Third-party sources are quoted as appropriate. EVIDEN is not responsible or liable for the content of the external sources including external websites referenced in this publication.

While care has been taken in gathering the data and preparing the Whitepaper EVIDEN does not make any representations or warranties on behalf of themselves or others as to its accuracy or completeness and expressly exclude to the maximum extent permitted by law all those that might otherwise be implied.

Neither EVIDEN nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. Eviden accepts no responsibility or liability for any loss or damage of any nature occasioned to any person as a result of acting or refraining from acting because of, or in reliance on, any statement, fact, figure or expression of opinion or belief contained in this Whitepaper. This Whitepaper does not constitute advice or promise of any kind.

Status of information contained in this NIS2 Whitepaper, in particular on member states transposition as of 30th June 2024. There will be continuous updates of this whitepaper, so in case of your interest, please subscribe our newsletter: eureg@eviden.com **)**

EVIDEN maintains its intellectual property rights in relation to this publication.

Contents

1 Executive summary

1.1 Introduction

The Network and Information Security Directive 2 (NIS2 Directive) is a significant piece of European Union (EU) legislation that aims to strengthen the cybersecurity posture of its economy. This whitepaper seeks to provide a deeper understanding of the NIS2 Directive, its implications, and its impact on businesses operating within the EU.

Our objective is to demystify the complexities of the NIS2 Directive and present it in a manner that is accessible and actionable for businesses. We aim to highlight the key requirements of the NIS2 Directive, the sectors, and entities it applies to, and the steps businesses need to take to ensure compliance.

Furthermore, this whitepaper will serve as a guide for businesses navigating the new cybersecurity landscape shaped by the NIS2 Directive. It will provide insights into the potential challenges and opportunities presented by the directive, and how businesses can turn these into competitive advantages while pursuing compliance.

This whitepaper is designed to be a solid basis for understanding the NIS2 Directive and a roadmap for achieving compliance. We hope that it will empower organizations to not only meet their legal obligations but also to enhance their real cybersecurity & resilience measures, thereby protecting their business reputation, operational continuity, and information security.

In case there is a need to quickly approach key elements NIS2 Directive in the form of questions and answers, please refer to Section 10.

1.2 Target Audience

The NIS2 Directive impacts a wide range of organisations (approx. 160 000 in EU) and its stakeholders, both external and internal. The primary target audience for this whitepaper includes executives accountable and professionals responsible for cybersecurity and risk management within their organizations, as well as those seeking consultancy services or adequate, proportional solutions to ensure compliance with this new EU Directive.
NIS2 compliance challenge addresses the following key stakeholders:

Board Members (i.e., called in NIS2 Directive “management bodies”) whether individual or collective body in charge of cybersecurity, business continuity, crisis management, physical security.

Chief Compliance Officers (CCO) or Heads of Compliance are crucial stakeholders in the NIS2 Directive implementation. Their role is critical in ensuring that organizations comply with the new cybersecurity regulations and requirements. They oversee the development and enforcement of internal policies and procedures that align with the directive’s obligations, including risk management measures, incident response, and breach notification protocols. They are responsible for assurance of proportionality principle while implementing NIS2.

Chief Information Security Officers (CISOs): As the primary defenders of an organization's network and information systems, CISOs play a key role in implementing and overseeing cybersecurity risk and protection measures, coordinate cybersecurity & cyber resilience awareness training to executives, employees, or suppliers This white paper provides them with essential insights and strategies to align their practices with NIS 2 Directive.

> NIS2 Compliance is not only a CISO job but management bodies job.
> There are no mentions of CISO in the NIS2 Directive

Chief Security Officers (CSOs): Responsible for the overall security strategy, CSOs together with CISOs must integrate both physical aspects of cybersecurity measures. The directive's comprehensive approach to cybersecurity risk management, physical- and cybersecurity incident response, crisis management is particularly relevant to their roles. CSOs can act liaison for implementation activities related to CER (Critical Entities Resilience) Directive which overlaps with NIS2 Directive critical sectors and Essential entities.

Chief Risk Officers (CROs), Risk and Insurance Managers: CROs are responsible for identifying, analysing, and mitigating organisation-wide risks. The NIS 2 Directive's emphasis on risk management measures and compliance assessments aligns with their mandate to protect the organization from a wide array of threats. Moreover, they should assist CISOs in determination of proper parameters for risk loss retention and risk transfer for cyber insurance policy and during cyber incidents if they trigger insurance loss adjustment activities.

Data Protection Officers (DPOs): being already challenged with ensuring compliance with data protection regulations, DPOs need to understand how the NIS2 Directive intersects with GDPR requirements.

Information Security Managers, Team Leaders, or Unit Mangers: They focus on the tactical or operational implementation of security policies, procedures, and collection respective evidence for demonstration of compliance.

Some of key stakeholders mentioned above are indispensable for NIS2 Directive to be addressed, adequately prioritised and to provide actionable action plan for closing potential compliance gaps or escalating evidence collection on timely basis. The measures discussed herein are designed to enhance cybersecurity resilience, ensuring that organizations are well-prepared to meet the new regulatory obligations.

1.3 Acronyms

In this whitepaper some of the acronyms are used which are listed in the Table 1.

Table 1 Acronyms

Acronym	Meaning
NISD, NIS1	Network and Information Systems Directive from 2016 predecessor of NIS2 Directive
NIS2	Network and Information Systems Directive 2 – subject of this Whitepaper
EE	Essential Entity
IE	Important Entity
ENISA	The European Union Agency for Cybersecurity
EU-CyCLONe	European Cyber Crisis Liaison Organisation Network
GDPR	General Data Protection Regulation
CER	Critical Entities Resilience or Resilience of Critical Entities Directive (EU) 2022/2557
DORA	Digital Operational Resilience Act Regulation (EU) 2022/2554
ECA	European Cybersecurity Act Regulation (EU) 2019/881
CRA	Cyber Resilience Act (current status: proposal in final proceeding).
CSIRT	Computer Security Incident Response Team
CERT	Computer Emergency Response (Readiness) Team
SOC	Security Operational Centre
EU, EU Member States, EU MS	27 Member States of European Union: Belgium, Bulgaria, Czechia, Denmark, Germany, Estonia, Ireland, Greece, Spain, France, Croatia, Italy, Cyprus, Latvia, Lithuania, Luxembourg, Hungary, Malta, the Netherlands, Austria, Poland, Portugal, Romania, Slovenia, Slovakia, Finland and Sweden.
EEA	European Economic Area is 27 EU Member States plus Iceland, Liechtenstein, and Norway. EEA does not include Switzerland. Sources and more details on EEA Relevance: Efta.int, European Parliament,

Source: Eviden's own elaboration.

2 NIS2 Directive Introduction

2.1 What is the NIS2 Directive

The NIS2 Directive formally identified as "**Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union**" is a legislative act that aims to achieve a high common level of cybersecurity across the European Union. EU Member States must ensure that organisations being in scope of this Directive, called **Essential Entities (EE)** and **Important Entities** (**IE)** take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems, and to prevent or minimize the impact of incidents on recipients of their services and on other services. The measures must be based on an all-hazards approach (holistic view of threat landscape).

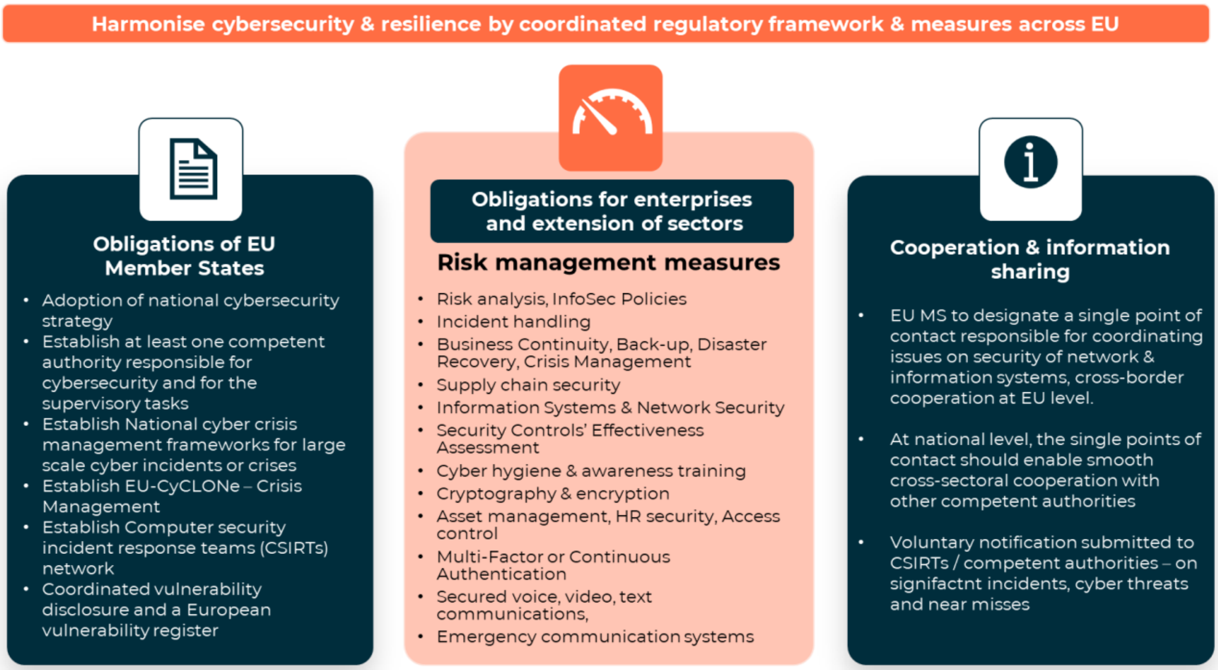
EU Member States authorities must until October 17th of October 2024 to transpose NIS2 Directive into national laws. Once adopted by EU countries, starting from 18th of October currently existing NIS1 Directive (NISD) will be replaced.

2.2 NIS2 Directive objectives & scope

The NIS2 Directive as strategic legislative initiative by the European Union aimed at elevating the level of cybersecurity across all member states. By understanding these objectives, businesses can better navigate the cybersecurity landscape shaped by the NIS2 Directive and take proactive steps towards not only compliance but also protection of their assets and value. Summary of NIS2 Directive main objective and specific objectives are depicted on Figure 1 Summary of NIS2 Directive key objectives and scope

.

Figure 1 Summary of NIS2 Directive key objectives and scope



Harmonise cybersecurity & resilience by coordinated regulatory framework & measures across EU

Obligations of EU Member States

- Adoption of national cybersecurity strategy
- Establish at least one competent authority responsible for cybersecurity and for the supervisory tasks
- Establish National cyber crisis management frameworks for large scale cyber incidents or crises
- Establish EU-CyCLONe – Crisis Management
- Establish Computer security incident response teams (CSIRTs) network
- Coordinated vulnerability disclosure and a European vulnerability register

Obligations for enterprises and extension of sectors

Risk management measures

- Risk analysis, InfoSec Policies
- Incident handling
- Business Continuity, Back-up, Disaster Recovery, Crisis Management
- Supply chain security
- Information Systems & Network Security
- Security Controls' Effectiveness Assessment
- Cyber hygiene & awareness training
- Cryptography & encryption
- Asset management, HR security, Access control
- Multi-Factor or Continuous Authentication
- Secured voice, video, text communications,
- Emergency communication systems

Cooperation & information sharing

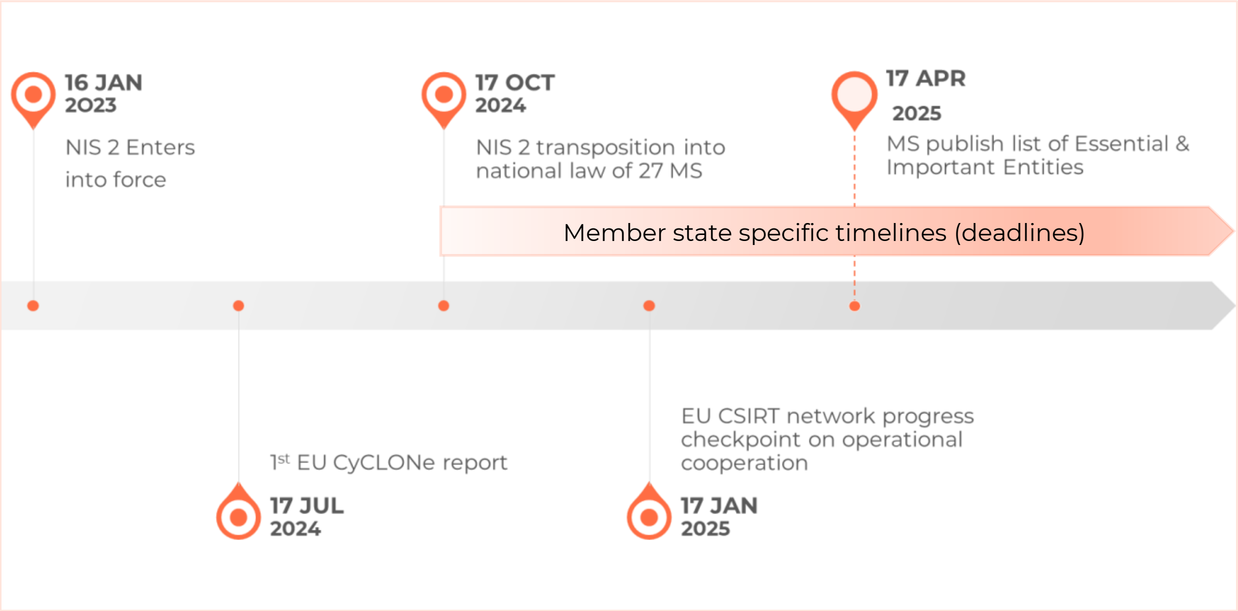
- EU MS to designate a single point of contact responsible for coordinating issues on security of network & information systems, cross-border cooperation at EU level.
- At national level, the single points of contact should enable smooth cross-sectoral cooperation with other competent authorities
- Voluntary notification submitted to CSIRTs / competent authorities – on signifactnt incidents, cyber threats and near misses

Source: Eviden's own elaboration based on NIS2 Directive.

2.3 NIS2 transposition and timeline

Although the NIS2 Directive is already in effect, EU Member States have until October 2024 to transpose it into national law. This transition period allows Member States to adopt and publish the necessary measures to comply with the directive and ensure that these measures are applied from 18 October 2024 onwards.

Figure 2 Key Milestones on NIS2 Compliance Journey


16 JAN 2023
NIS 2 Enters into force
17 OCT 2024
NIS 2 transposition into national law of 27 MS
17 APR 2025
MS publish list of Essential & Important Entities
Member state specific timelines (deadlines)
1st EU CyCLONe report
17 JUL 2024
EU CSIRT network progress checkpoint on operational cooperation
17 JAN 2025

2.4 Background of NIS2 Directive update

As already mentioned in section 2.1, NIS2 Directive is replacing previous NIS Directive (marked by NISD or NIS1 Acronyms). The EU cybersecurity rules introduced in 2016 were updated by the NIS2 Directive that came into force in January 2023. It modernized the existing legal framework to keep up with increased digitization and an evolving cybersecurity threat landscape. By expanding the scope of the cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities, and the EU as a whole.

The NIS2 directive introduces several key changes to enhance cybersecurity and the specific requirements that entities must adhere to.

NIS 1 or just NIS, was originally adopted in 2016 but the companies it applied to were limited, especially compared to NIS2. NIS also had minimal enforcement and much less punishing penalties for non-compliance.

What are the major differences between NIS and NIS2?

NIS2 carries much steeper fines and has detailed stricter rules and enforcement measures regulators must ensure companies are complying with NIS2. This includes investigative and supervisory powers such as:

- On-site inspections
- Security audits
- Requesting more information to assess an organization's cybersecurity measures.
- Security scanning
- Requesting evidence and information to measure risk management and cybersecurity policies, data, documentation, and other information.

Detailed comparison between NIS1 and NIS2 is shown in the Table below.

Table 2 Comparison between NIS and NIS2 Directives

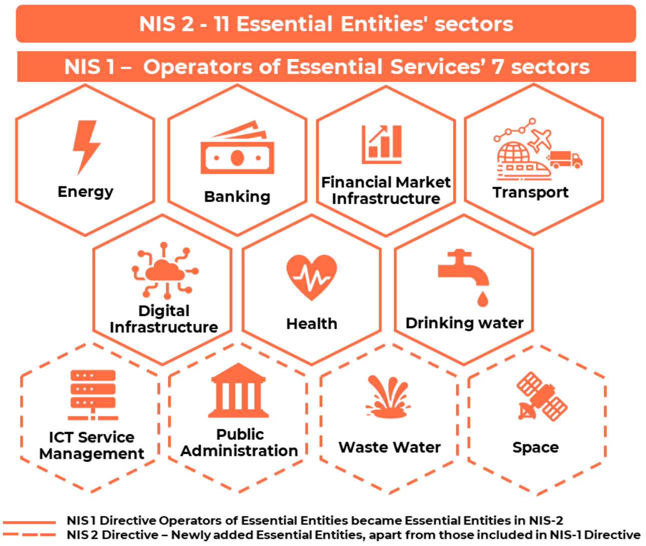
Difference Domain	NIS1 Directive	NIS2 Directive
Purpose	to build cybersecurity capabilities in EU mitigate threats to Network & IS used to provide essential services in key sectors ensure the continuity of such services when facing incidents, 7 sectors only contributing to the EU security and to the effective functioning of its economy & society	eliminate market fragmentation, enhance cross-border service provision, and improve cyber resilience affecting the cross-border provision of services and the level of cyber resilience to establish minimum rules for a **coordinated** regulatory framework effective cooperation among responsible authorities in each MS Extension the list of sectors from 7 to 18 overcome the shortcomings of the differentiation between operators of essential services and digital service providers
Types of organisations	Operators of Essential Services (OES) Digital Service Providers (DSP)	Essential Entities (EE) - OES in NIS1 Important Entities (IE)
Sectors in scope (see Figure 1 Summary of NIS2 Directive key objectives and scope)	7 critical sectors for OES 3 DSP sectors: Online marketplace. Online search engine. Cloud computing service	11 Critical sectors (all 7 from NIS1 and 1 DSP cloud service provider), 7 other critical sectors (incl. rest of NIS1 DSP plus social media platforms) EU MS can modify sectors in scope of NIS2
Measures	Different measures for OES (art. 14) and DSP (art. 16) – they are called Security requirements and incident notification	In NIS 2 measures are called risk management measures. They have more structured domains' measures (art. 21.2 a-j, 23) and are the same for EE and IE
Use of certification schemes	Not in scope, as European Cybersecurity Act has not been adopted at that time	Obligation to use certified products or services for Essential Entities
Audit by competent authority	**OES – required to provide:** - the information necessary to assess the security of their network and IS, including documented security policies as defined in Art 14. - evidence of the effective implementation of security policies, such as the results of a security audit conducted by the competent authority or a qualified auditor and, in the latter case, to make the results thereof, including the underlying evidence, available to the competent authority. **DSP – subject of ex post supervisory audit** DSP – required to provide: - the information necessary to assess the security of their network and information systems, including documented security policies - remediation to any failure to meet the requirements laid down in Art 16.	Essential Entity – subject of Ex ante and ex post – anytime, before, during and after cyber incident Important Entity – ex post, after cyber incident Important – ex post (audit only after the cyber incident) NIS2 introduced more detailed requirements here, refer to Section 3.2
Management accountability	No management bodies responsibilities defined or mentioned	Clear management bodies responsibilities, both legal entity and individuals

Difference Domain	NIS1 Directive	NIS2 Directive
Reporting	Incident notification obligations for OES, DSP. No incident report or no reporting timeline defined: for DSP (	Incident reporting in 24, 72 hours, interim and after 30 days (full report)
Administrative fines & penalties	No administrative fines' amount thresholds defined. Member States determine individually based on effective, proportionate, and dissuasive	Essential Entities 10 mln EUR or 2% of global turnover whichever is greater. Important Entities – 7 mln EUR or 1.4% of global turnover whichever is greater.

Source: Eviden's own elaboration. Country NIS1 transpositions introduced some modifications.
Note: Please refer to specific NIS1 Member States Transposition for further information.

Organisation in scope of NIS1 need to organise the transition to NIS2 based on respective mappings and extended scope of measures.

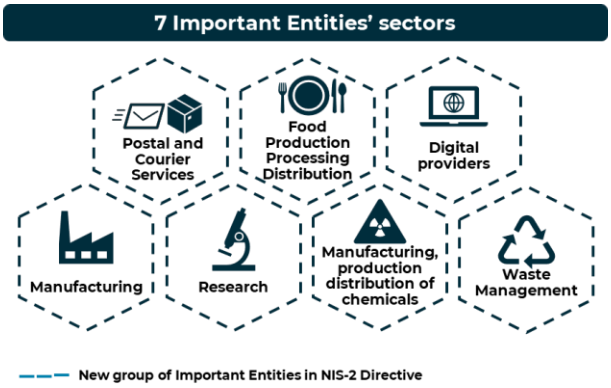
Figure 3 Comparison of Critical sectors between NIS1 (Annex I) of NIS2 directive (Annex I)


NIS 2 - 11 Essential Entities' sectors
NIS 1 – Operators of Essential Services' 7 sectors
Energy
Banking
Financial Market Infrastructure
Transport
Digital Infrastructure
Health
Drinking water
ICT Service Management
Public Administration
Waste Water
Space
NIS1 Directive Operators of Essential Entities became Essential Entities in NIS-2
NIS 2 Directive – Newly added Essential Entities, apart from those included in NIS-1 Directive

Source: Eviden's own elaboration

Digital providers from NIS1 have been assigned to Essential Entities (Cloud Service Provider) and the remaining ones to Important Entities.

Figure 4 Other critical sectors of NIS2 (Annex II)


7 Important Entities' sectors
Postal and Courier Services
Food Production Processing Distribution
Digital providers
Manufacturing
Research
Manufacturing, production distribution of chemicals
Waste Management
New group of Important Entities in NIS-2 Directive

Source: Eviden's own elaboration.

2.5 Does Companies in scope of NIS1 need to comply with NIS2?

Based on Section 2.3 of this whitepaper the following question emerges: "if organisations are already in NIS1 Directive scope, are they automatically compliant with NIS2?"

According to NIS2 Impact Assessment for the new organisations that would fall under the scope of the NIS framework, it is estimated that they would need an increase of maximum 22% of their current ICT security spending for the first years following the introduction of the new NIS framework

For companies being already under the scope of the current NIS 1 Directive, i.e. OES Operators of Essential Services) they would need on average 12% ICT spending increase).

In view of the above Table 2 Comparison between NIS and NIS2 DirectivesTable 2 – the NIS1 companies in view of NIS2 updated and precise requirements should consider:

- Address stricter governance of NIS2 compliance programme, management accountability and accountability for implementation and ongoing support of compliance
- Address necessity for regular training and cyber awareness of executives and employees
- Secure NIS2 compliance budget increase 10-20% of ICT Budget on average.
- Review current evidence collection and review process related to NIS2 risk management measures under Art. 21.2 a-j, in particular supply chain security, crisis management, zero trust scope and cyber hygiene.
- Review of incident reporting obligations process if it is able support generation of initial, interim, and full report under NIS2 time slots of 12, 72 and a one month since notification of incident.

For specific questions please consult Eviden local or global contact.

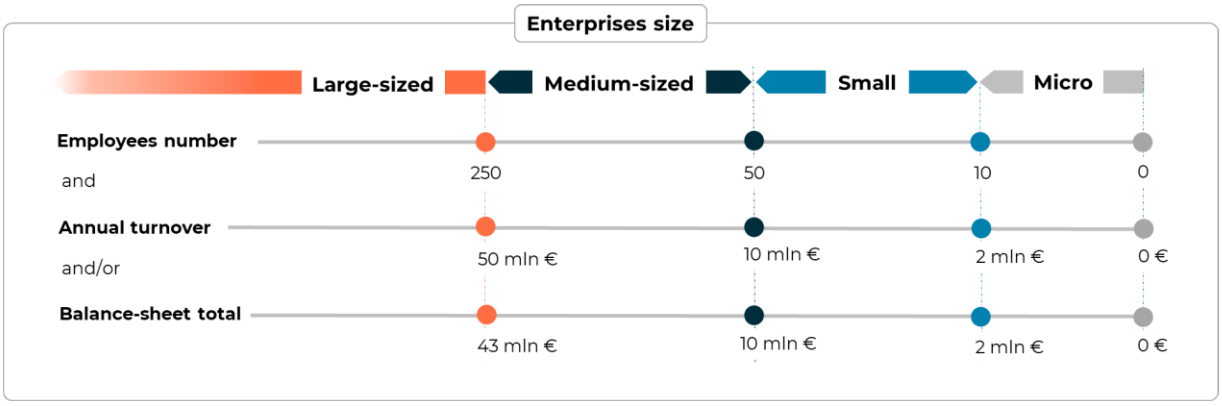
2.6 NIS2 Directive organisations in scope

2.6.1 Combined organisation size & sector criticality level

The NIS2 Directive extends and enhances the cybersecurity requirements for entities within the European Union, identifying sectors considered vital for the maintenance of societal and economic activities. This legislation distinguishes between "Essential Entities" and "Important Entities" to ensure a high common level of cybersecurity across the Union. The NIS2 Directive applies to organisations in critical sectors listed in its Annexes II and III, based on their size and the services they provide.

Art. 2 of NIS 2 Directive refers to Recommendation 2003/361/EC, where in art. 2 are defined differentiation criteria, thresholds between large, medium, small and microenterprises, companies large and medium.

Figure 5 Organisation size criteria used in NIS2 to combine with sectors Annex I, II to define EE & IE



Source: Own elaboration based on Recommendation 2003/361/EC.

Combining size of companies and list of critical or other critical sectors contained in Annex I and II of NIS2 Directive results in basis for identification of Essential or Important Entities what is presented in **Error! Not a valid bookmark self-reference.**.

Table 3 List of Essential and Important Entities combined with critical sectors (Annex I) and organisation size

SECTORS – ANNEX I	SUBSECTOR	LARGE ENTERPRISES	MEDIUM ENTERPRISES	SMALL & MICRO ENTERPRISES
Energy	Electricity, District heating and cooling, Oil, Gas and Hydrogen	🟠 **Essential Entities**	⚫ **Important Entities**	**Not in scope**
Transport	Air, Rail, Water and Road			
Banking	Credit institutions			
Financial market infrastructures	Operators of trading venues, Central counterparties			
Health	Healthcare providers, EU reference laboratories, entities carrying out research and development activities of medicinal products, entities manufacturing basic pharmaceutical products and pharmaceutical preparations and entities manufacturing medical devices considered to be critical during a public health emergency			
Drinking water	Suppliers and distributors of water intended for human consumption			
Digital infrastructure	Internet Exchange Point providers			
	DNS service providers, excluding operators of root name servers	🟠	🟠	🟠
	TLD name registries			
	Cloud computing service providers	🟠	⚫	**Not in scope**
	Data center service providers			
	Content delivery network providers			
	Trust service providers	🟠	🟠	🟠
	Providers of public electronic communications networks	🟠	🟠	⚫
	Providers of publicly available electronic communications services	🟠	⚫	**Not in scope**
Waste water	Undertakings collecting, disposing of or treating urban waste-water, domestic waste-water or industrial waste-water			
ICT service management (business-to-business)	Managed service providers and managed security service providers			
Public administration	Public administration entities of central governments	🟠	🟠	🟠
	Public administration entities at regional level	🟠	⚫	⚫
Space	Operators of ground-based infrastructure	🟠	⚫	**Not in scope**

Table 4 List of Important Entities combined with other critical sectors (Annex II) and organisation size.

SECTORS – ANNEX II	SUBSECTOR	LARGE ENTERPRISES	MEDIUM ENTERPRISES	SMALL & MICRO ENTERPRISES
Postal and courier services	Postal service providers	⚫ **Important Entities**	⚫ **Important Entities**	**Not in scope**
Waste management	Waste management companies			
Manufacture, production and distribution of chemicals	Companies involved in the manufacture of substances and the manufacture and distribution of substances or mixtures			
Production, processing and distribution of food	Wholesale distribution and industrial production and processing companies			
Manufacturing	Manufacture of medical devices and in vitro diagnostic medical devices			
	Manufacture of computer, electronic and optical products			
	Manufacture of electrical equipment			
	Manufacture of machinery and equipment n.e.c.			
	Manufacture of motor vehicles, trailers and semi-trailers			
	Manufacture of other transport equipment			
Digital providers	Providers of online marketplaces; online search engines and social networking services platforms			
Research	Research organisations			

Definitions of large, medium, small, and micro enterprises as in Recommendation 2003/361/EC and Figure 5.

2.6.2 Territory Jurisdiction Scope – Where to report, where to comply

According to Motive (113) and art 26 of NIS2 Directive, the entities falling within the scope of NIS2 should be considered to fall under the jurisdiction of the Member State in which they are established.

However, providers of public electronic communications networks or providers of publicly available electronic communications services should be considered to fall under the authority of the Member State in which they provide their services.

Specific technical suppliers:

- 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 and of social networking services platforms

should be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union.

Public administration entities should fall under the jurisdiction of the Member State which established them.

If the entity provides services or is established in more than one Member State, it should fall under the separate and concurrent jurisdiction of each of those Member States. The competent authorities of those Member States should cooperate, provide mutual assistance to each other and, where appropriate, carry out joint supervisory actions.

Where Member States exercise jurisdiction, they should not impose enforcement measures or penalties more than once for the same conduct, in line with the principle of ne bis in idem[1].

Multiple reporting obligations but only one penalty for the same conduct.

1. Jurisdiction and territoriality - According to article 26 of NIS2 – organisations in scope of this Directive are subject to the laws of the Member State where they are established. However, there are exceptions for the following entities:
    - Providers of electronic communications networks or services: They fall under the jurisdiction of the Member State where they offer their services.
    - Specific technology providers:
        - DNS service providers, TLD name registries,
        - entities providing domain name registration services,
        - cloud computing service providers,
        - data centre service providers,

[1] Non bis in idem (sometimes rendered *non-bis in idem* or *ne bis in idem*) which translates from Latin as 'not twice in the same [thing]', is a legal doctrine in a criminal law under which a person cannot be punished and be subject to several procedures twice for the same facts. In simple terms, the principle pursues to avoid double prosecutions and double punishments.

        - 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 DNS service providers, cloud computing services, content delivery networks, etc., are subject to the laws of the Member State where they have their main establishment in the European Union.
    - Public administration entities: They are governed by the laws of the Member State that established them.

2. Determining Main Establishment:
    - For entities mentioned in the exceptions (like specific technology providers), their main establishment is where decisions related to cybersecurity risk management are primarily made.
    - If that cannot be determined or if decisions are not made within the EU, the main establishment is where cybersecurity operations occur.
    - If still unclear, it is based on the Member State where the entity has the most employees.
3. Non-EU Entities Offering Services:
    - If a non-EU entity provides services within the EU, it must appoint a representative in one of the Member States where it operates.
    - Legal actions can be taken against such entities for violating this Directive.
4. Representatives and Legal Actions:
    - Appointing a representative does not protect the entity from legal actions—it is separate from any legal liability.
    - Legal actions can still be initiated directly against the entity itself.
5. Mutual Assistance and Enforcement:
    - Member States can take supervisory and enforcement measures if they receive a request for mutual assistance related to an entity covered by the exceptions. This is described in Art. 37: “In case of mutual assistance Where an entity provides services in more than one Member State or provides services in one or more Member States and its network and information systems are located in one or more other Member States, the competent authorities of the Member States concerned shall cooperate with and assist each other as necessary.”

2.6.2.1 NIS2 Jurisdiction scoping – Eviden’s experiences

Considering so far Eviden’s experience in NIS2 Customer Engagements Compliance Projects, the following options were identified:

1. Minimum scenario: organisation has EU based country Head Office and operates in one country only, Essential Entity or Important Entity - clear classic ("handbook") situation.

2. Maximum scenario: organisation operates in all or in most of the EU Member States or EEA (Economic European Area) – Countries’ subsidiaries with Head office being in one of EU member states. An additional complication in this case could be that in one EU country the organisation (entity) will be potentially recognized as an Essential Entity and in the other one as Important Entity. No subsidiaries outside the European Economic Area. Incident reporting may be doubled or multiplied dependent on its presence in the specific EU member states.

3. Like scenario in point 2, but Head office 1 EU member states country, Essential or Important Entity, business operates in all or in most of the EU Member States plus outside EU - subsidiaries outside EEA: in short partially subsidiaries in EU member states, partially outside EU or EEA.

4. Head office is outside EU/EEA but still there may be business operating in several EU based subsidiaries (or at least one subsidiary (especially of bigger multi-industry group from US, Canada etc.) what classifies them to be in scope of NIS2. This means in such situations the companies' subsidiaries would need to satisfy NIS2 requirements, but not necessarily its head office.

5. Company is already subject of NIS1 Directive from 2016 and needs transition activities mainly unless their territorial remains the same (no other EU MS expansion, etc.).

6. Company, apart from above cases may fall under CER Directive in the given country (all Essential Entities under NIS2 are Critical Entities under CER Directive. In view of that joint NIS2 and CER Directive compliance journey could be considered to leverage cost synergy of similar compliance challenges.

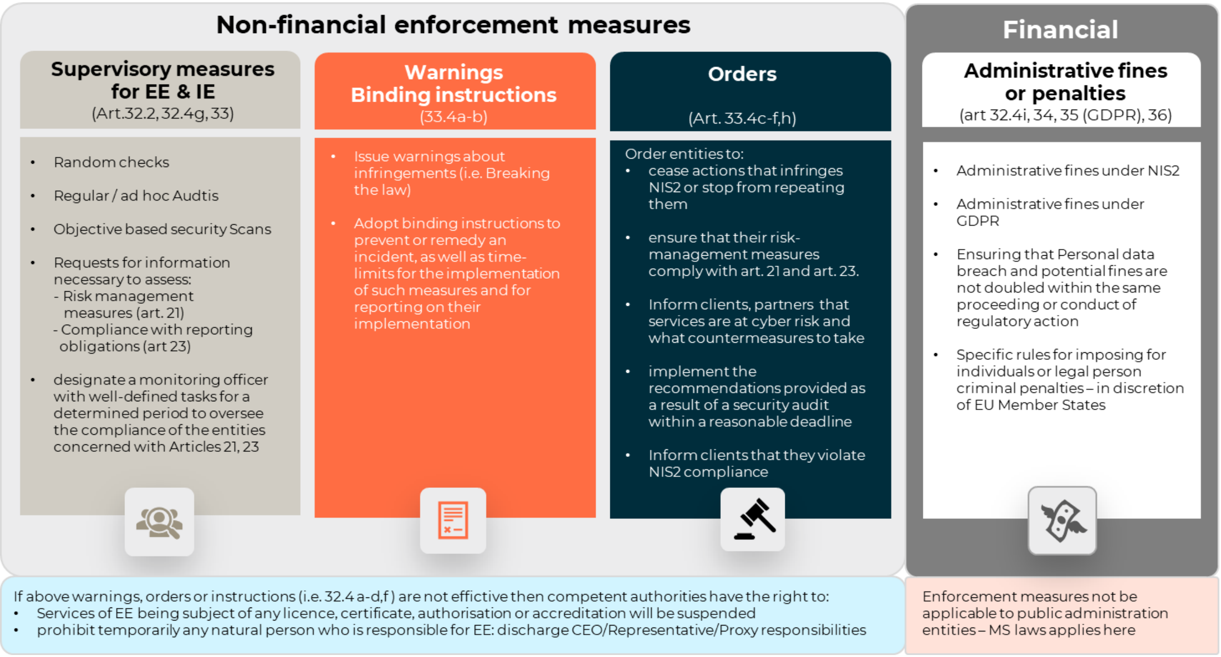
7. Non-governmental organizations outside the EU, but stakeholders expect compliance with EU NIS2, DORA, CRA, etc. Such cases refer to non-profit organizations located in Switzerland, Norway, Island which have suppliers with major business activity in EU member states.

3 NIS2 Supervisory & Enforcement Measures

3.1 General Overview of Types of Supervisory and Enforcement Measures

„Competent authority" is the term used in the NIS2 to refer to the regulatory authority which needs to be designated or adopted for each EU Member State. There are supposed to be many competent authorities responsible for the different sectors in scope of NIS2. These authorities have enforcement powers and can take the following supervisory measures (like random checks, audits, requests for information), warnings, orders, administrative fines, or penalties. which are depicted in the Figure 6.

Figure 6 Types of NIS2 Competent Authorities' Supervisory & Enforcement Measures



Non-financial enforcement measures

Supervisory measures for EE & IE
(Art.32.2, 32.4g, 33)

- Random checks
- Regular / ad hoc Audtis
- Objective based security Scans
- Requests for information necessary to assess:
  - Risk management measures (art. 21)
  - Compliance with reporting obligations (art 23)
- designate a monitoring officer with well-defined tasks for a determined period to oversee the compliance of the entities concerned with Articles 21, 23

Warnings Binding instructions
(33.4a-b)

- Issue warnings about infringements (i.e. Breaking the law)
- Adopt binding instructions to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation

Orders
(Art. 33.4c-f,h)

Order entities to:
- cease actions that infringes NIS2 or stop from repeating them
- ensure that their risk-management measures comply with art. 21 and art. 23.
- Inform clients, partners that services are at cyber risk and what countermeasures to take
- implement the recommendations provided as a result of a security audit within a reasonable deadline
- Inform clients that they violate NIS2 compliance

Financial

Administrative fines or penalties
(art 32.4i, 34, 35 (GDPR), 36)

- Administrative fines under NIS2
- Administrative fines under GDPR
- Ensuring that Personal data breach and potential fines are not doubled within the same proceeding or conduct of regulatory action
- Specific rules for imposing for individuals or legal person criminal penalties – in discretion of EU Member States

If above warnings, orders or instructions (i.e. 32.4 a-d,f) are not effictive then competent authorities have the right to:
- Services of EE being subject of any licence, certificate, authorisation or accreditation will be suspended
- prohibit temporarily any natural person who is responsible for EE: discharge CEO/Representative/Proxy responsibilities

Enforcement measures not be applicable to public administration entities – MS laws applies here

While discussing Figure 5 it is important to draw attention to criminal penalties related to individuals which NIS2 includes as new measures to hold top management personally liable and responsible for significant negligence in case of a security incident Namely, NIS2 allows Member State authorities to suspend organisation's managers personally liable if material negligence is proven after a cyber incident.

This includes ordering that organisations to publish their compliance violations and identifying in public statements the natural and legal person(s) responsible for the violation and its size.

And if the organisation is an essential entity, temporarily ban an individual from performing management positions in case of repeated violations.

These measures are designed to recognize C-level management accountable and to prevent from material ignorance in managing cyber risks. Specific penalties will vary depending on the Member State, but the Directive establishes a minimum list of non-financial supervisory and enforcement measures for breaches of the cybersecurity risk management and reporting obligations.

3.2 Auditing of Essential or Important Entities

In the NIS2 Directive, dependent on types of entities, there has been adopted so called *ex ante* and *ex post* approach to supervisory activities like regulatory audits, on-site inspections, requests for information, etc.

Essential Entities under art. 32 of NIS2 are subject to an **ex-ante and ex-post approach** to supervision (i.e., before the incident happens, during or after, i.e., at any time).

Important Entities under art. 33 of NIS2 are subject **ex-post** - supervisory authorities will only conduct investigations into these entities if there is evidence or information that they have infringed their NIS 2 obligations (art. 21 or 23 in particular).

Table 5 Types of supervisory measures for Essential or Important Entities

Essential Entities (EE) Ex ante & Ex post (art. 32.2)	Important Entities (IE) Ex post (art. 33.2)
a) on-site inspections and off-site supervision, including **random checks** conducted by trained professionals*	a) on-site inspections and off-site **ex post supervision** conducted by trained professionals;
b) **regular** and targeted security audits carried out by an independent body or a competent authority**	b) **[non-regular]** targeted security audits carried out by an independent body or a competent authority
c) ad hoc audits, including where justified on the ground of a significant incident or an infringement of this Directive by the essential entity	Not applicable for IE
d) For EE security scans based on objective, non-discriminatory, fair, and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned, For IE the same provision but indicated as c)	
e) requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Art 27.	d) requests for information necessary to assess, **ex post**, ... (then the same as for IE, but indicated as d)
f) requests to access data, documents, and information necessary to carry out their supervisory tasks	e) the same as for IE, but indicated as e)
g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.	f) the same as for IE, but indicated as f)

Source: Eviden's own elaboration.

Explanations to the Table:

* on-site inspections and off-site supervision, including the identification of weaknesses in databases, hardware, firewalls, encryption, and networks. Those inspections and that supervision should be conducted in an objective manner.

** b) shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information

Note: Country-specific supervisory activities after transposition into national laws may differ from those provided in NIS2 Directive.

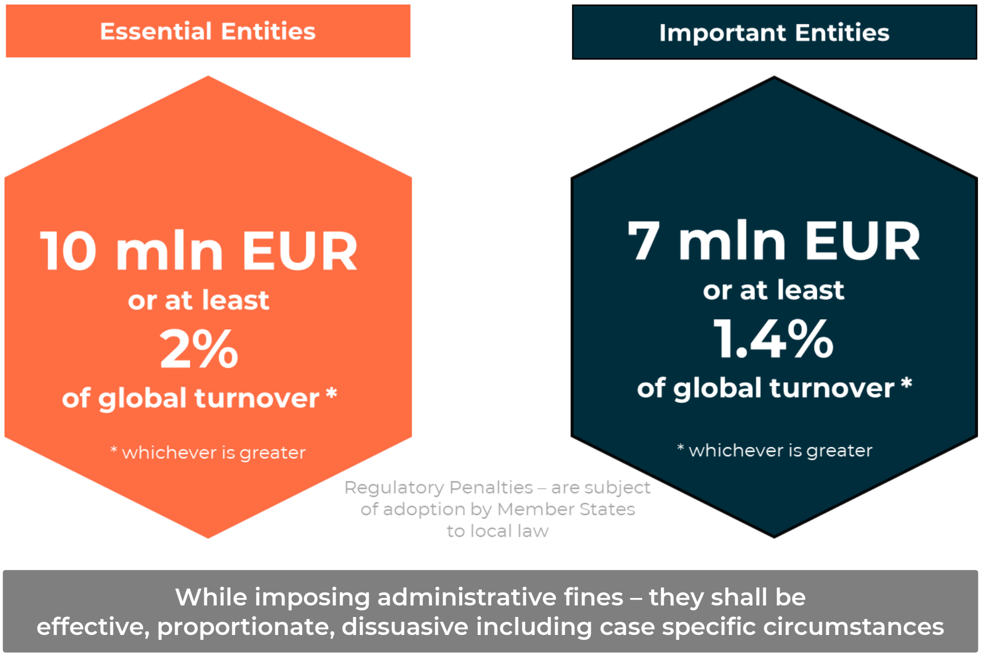
3.3 NIS2 Directive Penalties & administrative fines

Understanding the general conditions related to imposing potential administrative fines or penalties for non-compliance with NIS2 is crucial for organisations subject to the NIS2 Directive.

Member States shall ensure that in case of Essential Entities infringe Article 21 or 23 they are subject to administrative fines of a maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.

Member States shall ensure that in case of Important Entities infringe Article 21 or 23, important entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 7 000 000 or of a maximum of at least 1,4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.

Figure 7 Administrative fines in case of infringement of Article 21 or 23 by EE or IE.


Essential Entities
10 mln EUR
or at least
2%
of global turnover *
* whichever is greater
Important Entities
7 mln EUR
or at least
1.4%
of global turnover *
* whichever is greater
Regulatory Penalties – are subject of adoption by Member States to local law
While imposing administrative fines – they shall be effective, proportionate, dissuasive including case specific circumstances

According to motive (130) of NIS2 Where an administrative fine is imposed on an essential or important entity that is an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where an administrative fine is imposed on a person that is not an undertaking, the competent authority should take account of the general level of income in the Member State as well as the economic situation of the person when considering the appropriate amount of the fine. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines. Imposing an administrative fine does not affect the application of other powers of the competent authorities or of other penalties laid down in the national rules transposing this Directive.

According to motive (131) of NIS2 Member States should be able to lay down the rules on criminal penalties for infringements of the national rules transposing this Directive.

However, the imposition of criminal penalties for infringements of such national rules and of related administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice of the European Union.

According to motive (132) of NIS2 where NIS2 Directive does not harmonise administrative penalties or where necessary in other cases, for example in the event of a serious infringement of this Directive, Member States should implement a system which provides for effective, proportionate, and dissuasive penalties. The nature of such penalties and whether they are criminal or administrative should be determined by national law.

3.4 Mutual assistance in multi-country supervisory or enforcement measures

According to Art 37 of NIS2 in connection with Art. 26, where an Entity (Essential or Important) provides services in more than one Member State or provides services in one or more Member States and its network and information systems are located in one or more other Member States, the competent authorities of the Member States concerned shall cooperate with and assist each other as necessary.

That cooperation shall include at least:

- the competent authorities applying supervisory or enforcement measures in a Member State shall, via the single point of contact, inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken,

- a competent authority may request another competent authority to take supervisory or enforcement measures,

- a competent authority shall, upon receipt of a substantiated request from another competent authority, provide the other competent authority with mutual assistance proportionate to its own resources so that the supervisory or enforcement measures can be implemented in an effective, efficient, and consistent manner.

The mutual assistance referred above in the last listed point may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits.

A competent authority to which a request for assistance is addressed shall not refuse that request unless it is established that it does not have the competence to provide the requested assistance, the requested assistance is not proportionate to the supervisory tasks of the competent authority, or the request concerns information or entails activities which, if disclosed or carried out, would be contrary to the essential interests of the Member State’s national security, public security or defense.

Before refusing such a request, the competent authority shall consult the other competent authorities concerned and, upon the request of one of the Member States concerned, the Commission and ENISA.

Where appropriate and with common agreement, the competent authorities of various Member States may carry out joint supervisory actions over Essential or Important Entities operating in several EU member states under the conditions described above.

4 NIS 2 Directive Requirements and obligations

4.1 Introduction

There are two aspects of NIS2 compliance first is for Member States or EU Institution Compliance which will not be explored in this document and the second aspect is the one for identified entities and sectors. Core of the requirements are defined in NIS2 Art. 20, 21, 23 and 24 with partial reference also to Art 25.

The NIS2 Directive aims to enhance the cybersecurity framework within the European Union, building on the foundation set by the original NIS Directive. It introduces comprehensive measures to ensure robust governance, risk management, incident reporting, and adherence to EU cybersecurity certification schemes. The directive mandates that essential and important entities implement these measures to mitigate risks and improve resilience against cyber threats. This visual representation highlights the core areas of compliance: Governance (Art 20), Cybersecurity Risk Management Measures (Art 21), Reporting Obligations (Art 23), and European Cybersecurity Certification Schemes (Art 24).

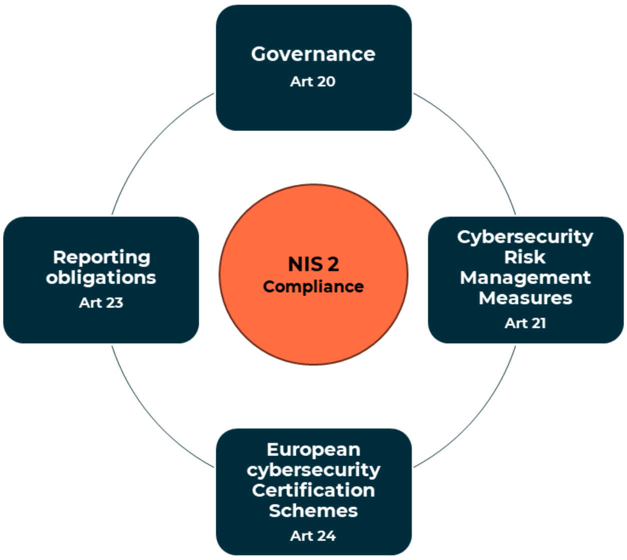

Governance
Art 20
Reporting obligations
Art 23
NIS 2
Compliance
Cybersecurity Risk Management Measures
Art 21
European cybersecurity Certification Schemes
Art 24

Figure 8 Summary of NIS2 Requirements categories per Article

4.2 Governance (Art. 20)

Article 20 of NIS2 Directive highlights the significance and responsibilities that governing bodies of organizations will acquire. It focuses on two points:

- The management bodies of **Essential** and **Important Entities** will be responsible for approving cybersecurity risk management measures and overseeing their implementation to comply with Article 21 and incident reporting requirements regarding Article 23.

- **Members of these management teams must attend periodic cybersecurity risk management training**. Similarly, employees, encouraged or obliged by the governing bodies, should also periodically acquire or update the knowledge and skills necessary. This ensures that employees have the necessary situational awareness and skills to identify potential risks and evaluate the effectiveness of cybersecurity practices and their influence on the organisation's services.

Article 20 Governance

The management bodies of essential and important entities:

- approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21,
- oversee its implementation and can be held liable for infringements by the entities of that Article.
- are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis,

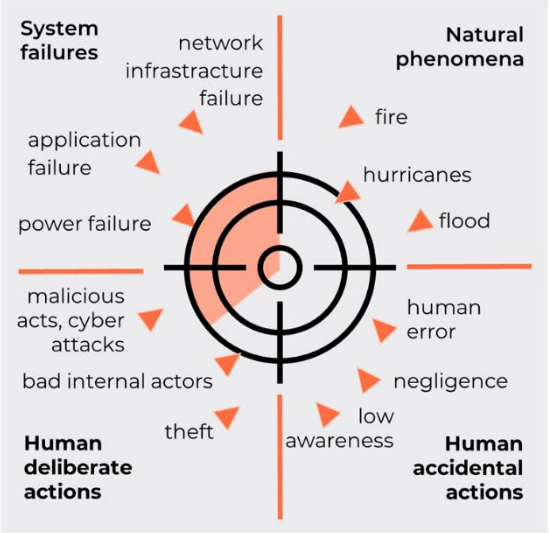
in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

4.3 Cybersecurity Risk Management Measures (Art. 21)

Administrative fines and penalties under NIS2 Directive refer to Article 21 and 23, which requires Member States to ensure that essential and important entities implement appropriate and proportionate technical, operational, and organizational measures. These measures aim to mitigate risks of the security of network and information systems used in their operations or service provision, and to minimize the impact of incidents on service recipients and other services. The proportionality of these measures should be assessed based on the state-of-the-art, relevant European and international standards, the cost of implementation, the entity's exposure to risks, its size, and the likelihood and severity of potential incidents, including their societal and economic impacts.

The measures should adopt an **all-hazards approach** (see Recital 79 of NIS2) to protect both network and information systems and their physical environments. All-hazards approach – anticipation of cybersecurity risks with real potential to become cybersecurity incidents coming from any direction.

Figure 9 Understanding All-hazards approach.



All-hazards approach in NIS2:

An all-hazards approach is an integrated preparedness approach to cyber related threats, incidents, emergencies or crises.

This approach focuses on capacities and capabilities that are critical to anticipation and preparedness for a full spectrum of cyber risk sources, attack vectors coming from any direction, agents, locations, etc, disasters, including internal emergencies and a man-made (deliberate or accidental actions) emergency (or both) or natural disasters.

It includes both virtual, logical and physical environments of information systems and networks.

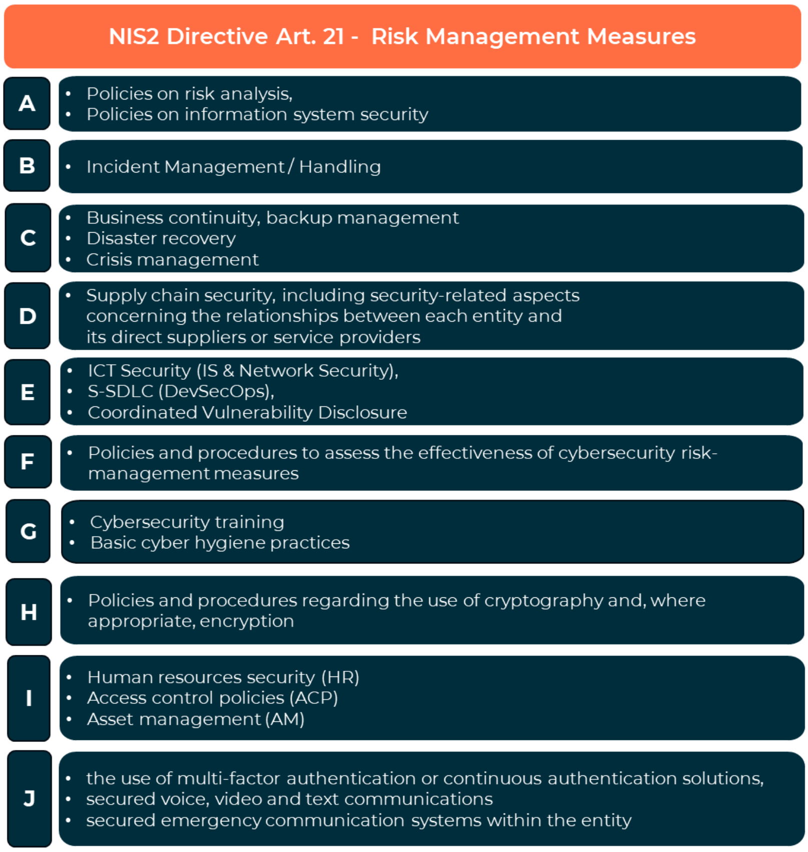
Source: Eviden’s own elaboration.

Organisation's cybersecurity & resilience strategy under NIS2 Directive needs to anticipate risks and incidents coming from any direction. This would include cyberattacks, natural disasters: fire, flood, strong winds, bad internal actors, negligence and many other potential incident vectors, theft, sabotage, telecommunication or power failures, or entity's information and information processing facilities, which could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems. The cybersecurity risk-management measures should therefore also address the physical and environmental security of network and information systems. .

In that regard, essential and important entities should, as part of their cybersecurity risk-management measures, also address human resources security and have in place appropriate access control policies. Those measures should be consistent with Directive (EU) 2022/2557.

NIS2 Risk Management Measures of Art. 21 are listed on Figure 10.

Figure 10 NIS2 Risk Management Measures



NIS2 Directive Art. 21 - Risk Management Measures	
A	• Policies on risk analysis, • Policies on information system security
B	• Incident Management / Handling
C	• Business continuity, backup management • Disaster recovery • Crisis management
D	• Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
E	• ICT Security (IS & Network Security), • S-SDLC (DevSecOps), • Coordinated Vulnerability Disclosure
F	• Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
G	• Cybersecurity training • Basic cyber hygiene practices
H	• Policies and procedures regarding the use of cryptography and, where appropriate, encryption
I	• Human resources security (HR) • Access control policies (ACP) • Asset management (AM)
J	• the use of multi-factor authentication or continuous authentication solutions, • secured voice, video and text communications • secured emergency communication systems within the entity

Source: Eviden's own elaboration based on art. 21.2. of NIS2 Directive.

In NIS2 these measures as listed as follows:
(a) Policies on risk analysis and information system security
(b) Incident handling
(c) Business continuity, such as backup management and disaster recovery, and crisis management
(d) Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
(e) Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure
(f) Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
(g) Basic cyber hygiene practices and cybersecurity training
(h) Policies and procedures regarding the use of cryptography and, where appropriate, encryption
(i) Human resources security, access control policies and asset management

(j) The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate
All member states are also tasked with ensuring that entities consider the vulnerabilities specific to each direct supplier and service provider, and the overall quality of products and cybersecurity practices, including secure development procedures.

4.4 Reporting obligations (Art. 23)

Administrative fines and penalties under NIS2 Directive, apart from Article 21 (Risk Management measures) also refer to Article 23 which is discussed in this section. Article 23 mandates that member states require organizations to report any significant disruptions to their service provision to the CSIRT or, if relevant, the competent authority. Additionally, if there is a significant cyber threat, organizations must inform the recipients of their services who might be affected, advising them of any actions or remedies they can undertake in response to the threat. Where applicable, organisations may also provide information about the threat itself to the recipients.

Article 23 reporting obligations: entities must notify the Computer Security Incident Response Team or applicable authority of:

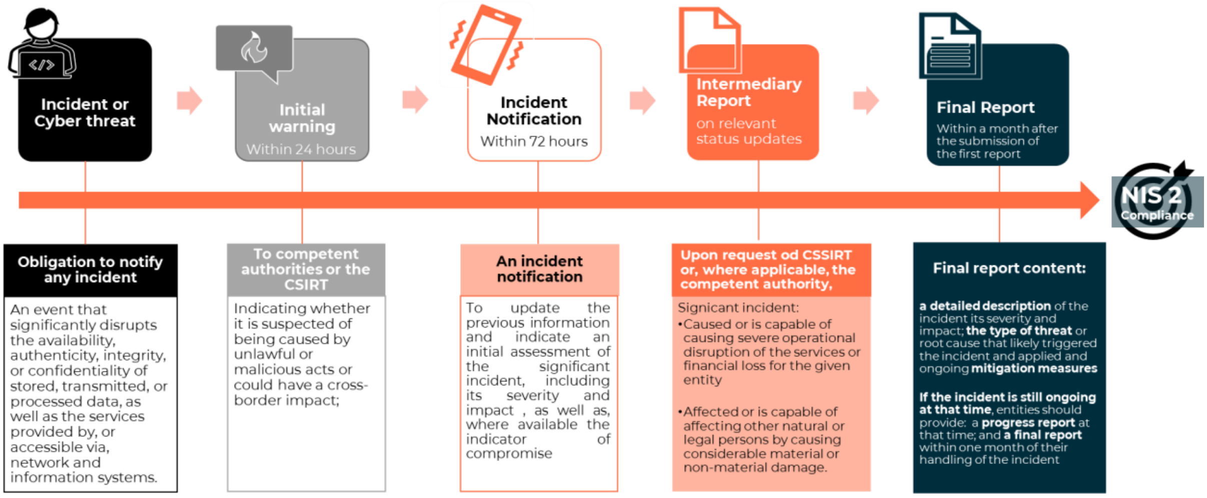
- Any incident / disruption that significantly impacts their ability to provide services.
- Any cross-border impacts of the incident (i.e., access to data by other CSP jurisdiction).

Article 23 reporting obligations: entities must notify the recipients of their services of:

- Significant incidents that are likely to adversely affect their ability to provide services.
- Significant cyber threats and any measures or remedies taken in response.

Key milestones of incident reporting obligations are presented on Figure 11.

Figure 11 Incident Reporting to Competent Authority



Obligation to notify any incident

An event that significantly disrupts the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data, as well as the services provided by, or accessible via, network and information systems.

To competent authorities or the CSIRT

Indicating whether it is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

An incident notification

To update the previous information and indicate an initial assessment of the significant incident, including its severity and impact , as well as, where available the indicator of compromise

Upon request od CSSIRT or, where applicable, the competent authority,

Signicant incident:

- Caused or is capable of causing severe operational disruption of the services or financial loss for the given entity
- Affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Final report content:

a detailed description of the incident its severity and impact; **the type of threat** or root cause that likely triggered the incident and applied and ongoing **mitigation measures**

If the incident is still ongoing at that time, entities should provide: a **progress report** at that time; and **a final report** within one month of their handling of the incident

Source: Eviden's own elaboration based on the NIS2 Directive

According to Motive 102 Where essential or important entities become aware of a significant incident, they should be required to submit an early warning without undue delay and in any event within 24 hours. That early warning should be followed by an incident notification.

The entities concerned should submit an incident notification without undue delay and in any event within 72 hours of becoming aware of the significant incident, with the aim, in particular, of updating information submitted through the early warning and indicating an initial assessment of the significant incident, including its severity and impact, as well as indicators of compromise, where available. A final report should be submitted not later than one month after the incident notification.

The early warning should only include the information necessary to make the CSIRT, or where applicable the competent authority, aware of the significant incident and allow the entity concerned to seek assistance, if required. Such early warning, where applicable, should indicate whether the significant incident is suspected of being caused by unlawful or malicious acts, and whether it is likely to have a cross-border impact.

Member States should ensure that the obligation to submit that early warning, or the subsequent incident notification, does not divert the notifying entity's resources from activities related to incident handling that should be prioritised, in order to prevent incident reporting obligations from either diverting resources from significant incident response handling or otherwise compromising the entity's efforts in that respect.

In the event of an ongoing incident at the time of the submission of the final report, Member States should ensure that entities concerned provide a progress report at that time, and a final report within one month of their handling of the significant incident.

4.5 Use of European cybersecurity certification schemes (Art. 24)

Article 24 of NIS2 outlines the use of European cybersecurity certification schemes to ensure compliance with specific requirements of Article 21. Member states may require essential and important entities to utilize certified ICT products, services, and processes. These certifications must adhere to European cybersecurity certification schemes established under Article 49 of Regulation (EU) 2019/881 (i.e. European Cybersecurity Act), whether developed internally by the entities or procured from third parties.

The European Commission has the authority to issue delegated acts, according to Article 38, to specify which categories of essential and important entities must use certain certified ICT products, services, and processes, or obtain certification under a European scheme as per Article 49 of Regulation (EU) 2019/881. These acts will be adopted when cybersecurity levels are deemed insufficient and will include a specified implementation period. The Commission will perform impact assessments and consultations in line with Article 56 of Regulation (EU) 2019/881 before adopting these delegated acts.

In instances where an appropriate European cybersecurity certification scheme does not exist, the Commission may consult with the Cooperation Group and the European Cybersecurity Certification Group and request EVIDEN to develop a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881.

4.6 Standardisation (Art. 25)

According to art. 25 of convergent implementation of Article 21.1 and 21.2 of NIS2, there is obligation for Member States to encourage use of European and international standards and technical specifications relevant to the security of network and information systems.

We could expect similarly to NIS1 Directive that ENISA will prepare guidelines regarding the technical areas of Art. 21.1/2 as well as regarding already existing standards, including national standards, which would allow for those areas to be covered.

Eviden's Team of Experts has already identified all relevant ISO, NIST, ISA and other International or European Standards, Technical Specifications, ISO Technical Reports or Guidelines applicable to NIS2 requirements addressed in art. 20, 21 and 23. Therefore there is no need to wait until those standards are published, as there are already some countries transposed Directive, and indicating on certain standards family.

Eviden's experts mapped numerous standards to NIS2 requirements according to postulate of state-of-the-art risk management measures (Motive 62[2] (as obligation for ENISA), Motive 81[3] and corresponding art 21.1[4] (as obligation for Essential and Important Entities) which address and cover requirements in NIS2 directive. Those mapping were input data for elaboration various compliance gap analysis checklists or reflect them in the used supporting software solutions or tools.

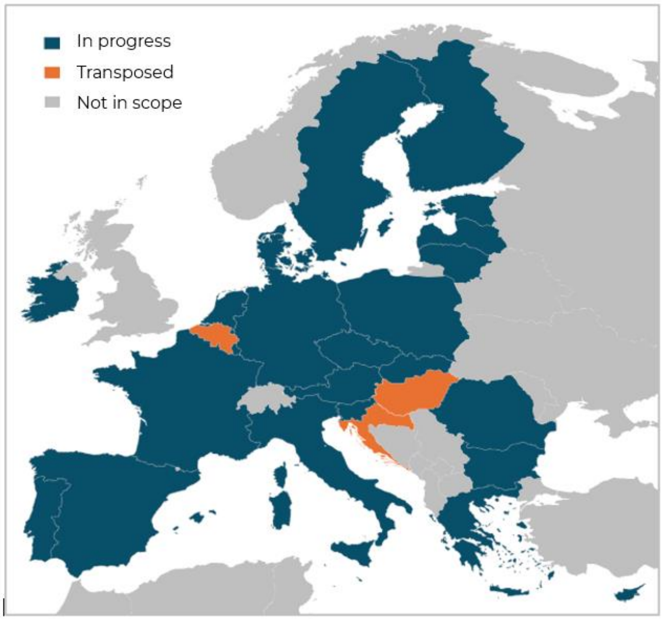
Please refer to Section 7 Eviden's approach to NIS2 compliance journey for further information.

5 EU Member States Progress in NIS2 Directive Transposition

Eviden's Team is monitoring the progress of into NIS2 Directive transposition into EU member states national laws. As of publication date of this whitepaper only 3 countries fully transposed the directive: Belgium, Croatia, and Hungary. With progress of transposition this whitepaper will updated.

Respective status is shown on the Figure 12.

Figure 12 NIS2 Directive Transposition Status across EU Member States.



Source: Eviden's own research. Transposed NIS2 Directive status is subject to change in the next months. Please consult Eviden's experts for current status. Legal acts are as they were publicly available at the moment of publication of this Whitepaper.

Selected key information on progress in some of the EU member states is given in the Table 6 Details on NIS2 Directive Transposition in selected Member States (alphabetically)Table 6.

[2] Access to correct and timely information about vulnerabilities affecting ICT products and ICT services contributes to an enhanced cybersecurity risk management. Sources of publicly available information about vulnerabilities are an important tool for the entities and for the users of their services, but also for the competent authorities and the CSIRTs. For that reason, ENISA should establish a European vulnerability database where entities, regardless of whether they fall within the scope of this Directive, and their suppliers of network and information systems, as well as the competent authorities and the CSIRTs, can disclose and register, on a voluntary basis, publicly known vulnerabilities for the purpose of allowing users to take appropriate mitigating measures. The aim of that database is to address the unique challenges posed by risks to Union entities. Furthermore, ENISA should establish an appropriate procedure regarding the publication process to give entities the time to take mitigating measures as regards their vulnerabilities and employ state-of-the-art cybersecurity risk-management measures as well as machine-readable datasets and corresponding interfaces. To encourage a culture of disclosure of vulnerabilities, disclosure should have no detrimental effects on the reporting natural or legal person.

[3] In order to avoid imposing a disproportionate financial and administrative burden on essential and important entities, the **cybersecurity risk-management measures should be proportionate to the risks posed to the network and information system concerned, taking into account the state-of-the-art of such measures**, and, where applicable, relevant European and international standards, as well as the cost for their implementation.

[4] Considering the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size, and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

Table 6 Details on NIS2 Directive Transposition in selected Member States (alphabetically)

Member State	Country name of legal act which is transposed NIS2 Directive	Key country specific information
Austria	Draft published of NIS2 Transposition into Austrian law: „Entwurf Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024). With NIS2 transposition in Austria Telecommunication Law and Health Telematics law will be chagned (das „Telekommunikationsgesetz“ from 2021 „Gesundheitstelematikgesetz“ from 2012)	Art. § 32. (4) refers to Appendix 3 (Anlage 3) with extended (more detailed) specified risk management measures.
Belgium	NIS2 Transposed to Belgian law on 26 AVRIL 2024. - Loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique[5]	26-04-2024 Date of adoption. Art.30.3.1-10 same as in art. 21.2a)-j) of NIS2 plus added 11th measure: Coordinated Vulnerability Disclosure Policy Centre for Cybersecurity Belgium (CCB) developed Cyber Fundamentals Framework mapped to NIST CSF, CIS (SANS TOP 18) Controls, ISO 27001/2, ISA 62443 and where entities are classified based on the severity threat level for the industry with starting level as ‘small’ and 3 assurance levels: basic, important, essential.
Croatia	NIS2 Transposed to Croatian Law as NN 14/2024 with date 7.2.2024: Zakon o kibernetičkoj sigurnosti Croatia’s Cybersecurity Act (CCA) The Cybersecurity Act has been published in the Official Gazette of the Republic of Croatia and entered into force on 15 February 2024.	15-02-2024 Date of adoption. Extension of deadline for NIS2 compliance until February 2026. Art.30.1 of CCA same as in art. 21.2a)-j) of NIS2 Supervision for essential entities must be performed every 3 to 5 years. A cybersecurity audit for essential entities must be performed at least once every 2 years. Cybersecurity self-assessment for important entities must be performed at least once every 2 years.
France	Draft law published of NIS2 transposition to French law.	ANSSI defined 20 objectives to cover risk management measures of Art.21.2a)-j) of NIS2.
Germany	Draft law published of NIS2 Transposition into German law: Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung.	Art.30.2 of same as in art. 21.2a)-j) of NIS2 in the German Draft Law. Integration with KRITIS (Critical Infrastructure) sectors.
Hungary	NIS2 transposed to Hungarian law in 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről)(Act on Cybersecurity Certification and Cybersecurity Supervision) commenced on May 23, 2023, after the draft law underwent its consultation phase in February. This was followed by additional government decrees and a draft outlining the specific security measures, which underwent consultation in February 2024.	23-05-2023 Date of adoption of NIS2 Transposed Law. §§ 19, 20 are addressing Risk Management measures which are slightly different not fully mapped to in original NIS2 Directive, lacking phrase of “supply chain” (procurement is used instead) and multifactor authentication and cyber hygiene elements, crisis management. Public transport: rail and road passenger transport, added as new sector.

[5] As for Belgium there is also Niderlandish version of NIS2 - (26 APRIL 2024. - Wet tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid)

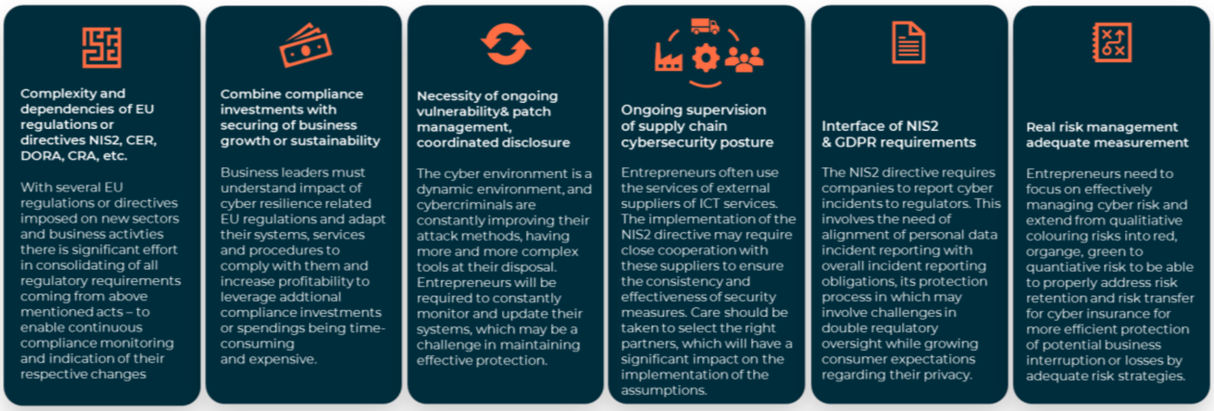
Member State	Country name of legal act which is transposed NIS2 Directive	Key country specific information
	A Hungarian government decree (Government Decree 305/2023 (VII. 11.) on the amount of cybersecurity fines, detailed rules of procedure for the imposition and payment of fines). Further sections of the NIS2 implementation will become effective by October 2024. For affected entities, there are some deadlines in 2024, starting with registration in June.	
Poland	Draft law published of NIS2 Transposition into Polish law: Ustawa o Krajowym Systemie Cyberbezpieczeństwa (UKSC) („Act for National Cybersecurity System") - draft as of 23-04-2024).	Art. 8, 9, 10 contain risk management measures mostly the same of Art.21.2a)-j) of NIS2, however some elements are missing like crisis management, back-up in comparison to original directive. Also "thematic policies" apart from policies on risk analysis and information security are added. In draft transposing NIS2 into Polish law, there are more essential entities sectors than in original NIS2 Directive: Manufacturing, Chemicals, Food (they were moved from other critical sectors (Annex II) to Annex I, and consequently from IE to EE Group. In draft law of NIS2 Directive ISO/IEC 27001, ISO/IEC 22301 certification is proposed to be sufficient measures to address NIS2 compliance.

Source: Eviden's own research

6 NIS2 compliance challenges for the enterprises

Entrepreneurs who are obliged to implement relevant requirements indicated by NIS2 Directive must face several challenges, therefore they should rethink their current cybersecurity & business resilience strategy, investments financing it to assure its execution with sufficient resources. Adoption of risk management measures will require joint & close cooperation between subject matter experts in the field of cybersecurity, resilience, business and legal. Overview of exemplary challenges for organisations are highlighted on Figure 13.

Figure 13 NIS2 Requirements Implementation challenges and business impacts



Complexity and dependencies of EU regulations or directives NIS2, CER, DORA, CRA, etc.

With several EU regulations or directives imposed on new sectors and business activties there is significant effort in consolidating of all regulatory requirements coming from above mentioned acts – to enable continuous compliance monitoring and indication of their respective changes

Combine compliance investments with securing of business growth or sustainability

Business leaders must understand impact of cyber resilience related EU regulations and adapt their systems, services and procedures to comply with them and increase profitability to leverage addtional compliance investments or spendings being time-consuming and expensive.

Necessity of ongoing vulnerability& patch management, coordinated disclosure

The cyber environment is a dynamic environment, and cybercriminals are constantly improving their attack methods, having more and more complex tools at their disposal. Entrepreneurs will be required to constantly monitor and update their systems, which may be a challenge in maintaining effective protection.

Ongoing supervision of supply chain cybersecurity posture

Entrepreneurs often use the services of external suppliers of ICT services. The implementation of the NIS2 directive may require close cooperation with these suppliers to ensure the consistency and effectiveness of security measures. Care should be taken to select the right partners, which will have a significant impact on the implementation of the assumptions.

Interface of NIS2 & GDPR requirements

The NIS2 directive requires companies to report cyber incidents to regulators. This involves the need of alignment of personal data incident reporting with overall incident reporting obligations, its protection process in which may involve challenges in double requlatory oversight while growing consumer expectations regarding their privacy.

Real risk management adequate measurement

Entrepreneurs need to focus on effectively managing cyber risk and extend from qualitiative colouring risks into red, organge, green to quantiative risk to be able to properly address risk retention and risk transfer for cyber insurance for more efficient protection of potential business interruption or losses by adequate risk strategies.

Source: Eviden's own elaboration

Multidisciplinary Eviden Team is collecting above challenges as voice of the customer program to consolidate knowledge sharing and increase awareness within international teams worldwide for optimal serving the clients.

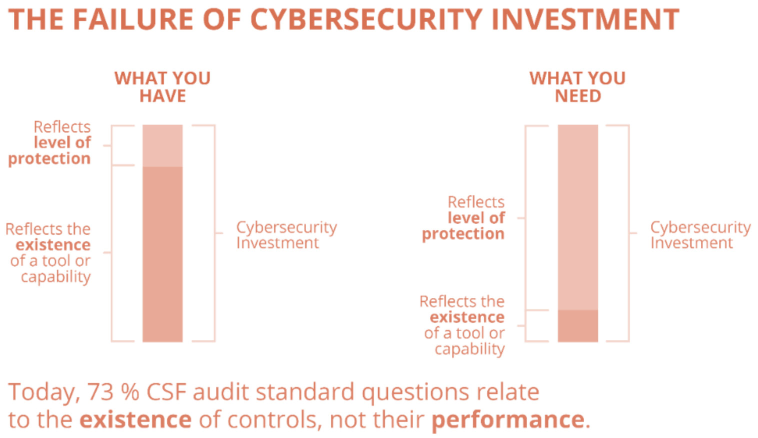
One of the most important activities related to NIS2 compliance is proper and adequate understanding of risk management measures as defined in Art. 21 and role of various supporting frameworks or standards.

We would like to draw your attention to the fact that various compliance schemes might be creating an impression by leading to controls being "compliant" (existing) instead of being 'effective,' i.e., working according to defined objectives for the specific control / safeguard. Such compliance activities will not increase cyber security posture or resilience of organisations in scope of NIS2.

In 'ENISA NIS Investments' report 2021 reference was made to Gartner's latest Emerging Risks Monitor Report that information security controls failure was listed as one the top emerging risk, after COVID-19 at that time. This observation is support by survey results shown on Figure 14.

Figure 14 Failure of cybersecurity investments due to main focus on control's existence

Figure 12: Cybersecurity controls – existence vs performance


THE FAILURE OF CYBERSECURITY INVESTMENT
WHAT YOU HAVE
Reflects level of protection
Reflects the existence of a tool or capability
Cybersecurity Investment
WHAT YOU NEED
Reflects level of protection
Reflects the existence of a tool or capability
Cybersecurity Investment
Today, 73 % CSF audit standard questions relate to the existence of controls, not their performance.

Source: Garner Emerging Risk Report in ENISA NIS Investments report https://www.enisa.europa.eu/publications/nis-investments-2021/@@download/fullReport

To assess the maturity of an organisation, existence of cybersecurity framework (CSF) controls or tooling does not necessarily imply a high level of cybersecurity maturity, their performance and effectiveness are more appropriate measures.

Similarly, focusing on products, solutions coverage, or managed security service instead of how those products contribute to increase controls effectiveness and performance is critical in generation overspending or overinvestment without increasing cybersecurity posture and security level resulting from efficient controls people, organizational, technical, or legislative.

To avoid not adequate investments in NIS2 compliance measures, controls, systems, platforms, processes during investment decision process special care should be put detailed justification of information on how new investment justifies limitations or lack of current controls performance & effectiveness gap vs new investments value added to controls effectiveness and performance. With this in mind investments will be proper allocation of funds not only for compliance but for real improvements of organisation's resilience.

Additional aspect of overspending or overinvesting and not achieving increase of cybersecurity level is commonly identified problem of relevant measurement of cyber risks, cybersecurity activities and trade-off against acceptable business risk, trade-off between spending and achieved value in protection.

Eviden Team has competences to assist organisations in this process to assure that NIS2 investments are adequately addressed.

6.1 NIS2 measures and cyber threat landscape – is this all real?

Apart from the aspects of proper investments in compliance some doubts might arise especially in new organisations in NIS2 scope or even in current ones under NIS1 on why more stricter and demanding requirements were imposed on them by NIS2. Natural question arises here whether there are the threats real, or is the impact of cybersecurity attack can be that big on current societies, states, or EU economy?

The answer is yes but it may have more or less different meaning dependent on sector, location and specific company profile of process or services and range of markets, specific organisations operate in. Therefore, in this place we highlight from the recent research, impacts of cyber-attacks on business per each industry defined in NIS2 Directive.

Of course, one must remember that country transposition of the NIS2 may result in additions of sectors or transfer several sectors from other critical (mainly for important entities) to be moved in critical sector and becoming essential entity (such situation applies to Polish draft of NIS2 transposition where food, manufacturing, and chemical are assigned to critical sectors).

In the Table 7 and Table 8 we consolidated key information cyber threats and its impact for the sectors in scope of NIS2 and respective NIS2 risk management measures to endorse implementation and prioritisation of NIS2 art 21 in relation to key impacts of cyber threats per industry with our recommendations to be careful and diligent regarding adequate investments in controls, products and services.

Table 7 Overview of research on real cybersecurity threats in critical sectors of Essential Entities

Specific NIS2 Critical Sectors impacts (Essential Entities)	Industry specific threats or disruptions (pains)	Applicable NIS2 Risk management key measures & actions
Energy Physical damage of pipelines, grids. Power black-out	Sabotage (physical damage) Attacks on ICS/SCADA systems Ransomware attacks Supply chain attacks Insider threats Phishing campaigns	IS & Network Lifecycle Security, in particular OT Security OT incident management Business Continuity Supply Chain Physical security (in connection with CER Directive) Human resources, employees background checks
Banking Interruption in customers funds availability, Theft of money	Phishing and social engineering Advanced Persistent Threats (APTs) Ransomware attacks Data breaches DDoS attacks	Cyber awareness both clients and employees Business Continuity Supply Chain Encryption Digital Operational Resilience Testing (see DORA Regulation)
Financial Market Infrastructure Stock Exchange quotations suspension, Lack of funds settlements	Cyberattacks on trading platforms Data integrity attacks Third-party service provider vulnerabilities Insider threats and fraud DDoS attacks	Business Continuity Supply Chain (Third Party Risk Management in DORA Regulation) Digital Operational Resilience Testing (see DORA Regulation) Encryption Incident Management
Transport Taking over of control of connected vehicles leading to road, water, air accidents Physical theft of vehicles with transported goods Stopping of transport booking systems (e.g. airlines and railways) disrupt their access to emergency and passenger systems services, and expose highly	Sabotage (hacking communication systems, physical damage of railway tracks) Cyberattacks on navigation systems Ransomware attacks Data breaches Attacks on connected vehicles to enable physical theft or data transfer GPS spoofing and jamming	Business continuity in the aspect of physical security of office, data centre, factory perimeter. IS & Network Lifecycle Security, in particular OT Security Products Lifecycle security, Connected vehicle security.

Specific NIS2 Critical Sectors impacts (Essential Entities)	Industry specific threats or disruptions (pains)	Applicable NIS2 Risk management key measures & actions
sensitive data causing mass chaos, and injuries or loss of life		
Drinking Water -Water poisoning putting people life at risk - interruptions to water distribution, treatment or storage - damage to pumps and valves, water tank overflow - alteration of chemical levels to hazardous amounts - switch to manual control - theft of customer's personal or billing data - cascading domino impact on sectors where continuous water is indispensable (hydroelectric facilities) the malfunction of passenger information screens, the disruption of applications used by railway staff through tablets, the suspension of all rail freight thus impacting shipments.	Cyber-physical attacks Ransomware attacks Data breaches Insider threats Phishing attacks	Business continuity in the aspect of physical security of office, data centre, factory perimeter. Human resources, employees background checks Business Continuity IS & Network Lifecycle Security
Health 800 medical operations of patients rescheduled due to ransomware in hospitals Blood test delayed Patients' health data, insurance numbers leakage	1st in the US Ransomware attacks on healthcare providers Data breaches Phishing attacks Attacks on medical devices Supply chain vulnerabilities	Personal Health Information IS & Network Lifecycle Security: IoT/OT Devices Security Human resources, employees background checks Business Continuity & Supply Chain Security Crisis Management
Digital Infrastructure	Cyberattacks on cloud services Data breaches DDoS attacks Supply chain attacks Insider threats	IS & Network Lifecycle Security Supply Chain, Cloud Security Human resources, employees background checks Business Continuity & Supply Chain Security Crisis Management
Public Administration Public services paralysed not available identity, municipal funds not received, health insurance payments, etc. Influencing elections, Disinformation of official government communication	Espionage and cyberattacks Ransomware attacks Phishing campaigns Data breaches DDoS attacks on public sector websites	IS & Network Lifecycle Security Supply Chain, Cloud Security Human resources, employees background checks Business Continuity & Supply Chain Security Crisis Management MFA and Secured Voice and Video Communication

Sources: Consolidated key information from cybersecurity landscape reports. Sources in Section 12.

Table 8 Overview of research on real cybersecurity threats in sectors of Important Entities

Specific NIS2 Other critical sectors impacts (Important Entities)	Industry specific threats or disruptions (pains)	Applicable NIS2 Risk management key measures & actions
Manufacturing Disclosure, tampering with, destruction or deletion of information in the manufactured products Stopping assembly line	Espionage and cyberattacks Ransomware attacks Phishing campaigns Supply chain attacks	& Network Lifecycle Security Supply Chain, Cloud Security Human resources, employees background checks Cyber awareness and cybersecurity posture of suppliers
Waste Water Poisoning of environment due to overflow of wastewater People health, safety or life impact on the impacted areas	Cyber-physical attacks Ransomware attacks Data breaches Insider threats Phishing attacks	IS & Network Lifecycle Security Supply Chain, Cloud Security Human resources, employees background checks Business Continuity & Supply Chain Security Crisis Management
Space	Cyberattacks on satellite control systems Data breaches involving mission data	IS & Network Lifecycle Security Supply Chain, Cloud Security Human resources, employees background checks

Specific NIS2 Other critical sectors impacts (Important Entities)	Industry specific threats or disruptions (pains)	Applicable NIS2 Risk management key measures & actions
Taking over control over satellites causing changing its direction leading to incidents or injuries or malfunction of satellite dependent infrastructure or industries Overheating of satellite leading to kinetic boom and physical damage GPS services, time stamp degradation Most invasive economic effect will result from the sudden unavailability of timestamps. Indeed, precise timing and time synchronisation, and frequency coordination (syntonisation) is used most notably in broadcasting and communications, including both cell phones and traditional telephone applications and the internet, so packets arrive at the same time in financial services for timestamping transactions.	Jamming and spoofing attacks Insider threats Supply chain attacks compromising space components Absence of navigation tools will be invasive in several sectors, such as: - In aviation, for monitoring positions of aircraft and satellite-based augmentation systems - Railroad train pacing systems for cruise control, positive train control to keep track of train location and movement authorities - In marine transportation, for navigation, collision avoidance, communications, and situational awareness - In vehicles, with handheld and embedded devices for navigation and fleet management.	Business Continuity & Supply Chain Security Crisis Management MFA and Secured Voice and Video Communication
Postal and Courier Services Paralysis of country ability to send letters and packages anywhere or abroad dependent on scope of the attack, impacting small exporters. Overtime cost for couriers and postmasters due to manual parcels, or official letters handling. Impact on court proceedings using still formal letters to notify about the date of trial, postponing the trials. Impact on insurers of parcels.	Ransomware attacks Data breaches Supply chain attacks Phishing attacks	Incident management, reporting even minor intrusions, as they could be the start of reconnaissance for something much bigger. Supply chain, security ICT Lifecycle security (DevSecOps)
Food production, processing, distribution Outage of connected systems for everything from tractor autosteer systems to crop moisture testing to automated distribution warehouses. Stoppage or slowdown during harvest season, for example, can reverberate throughout the entire industry as food processing plants and distribution networks feel the effects of events that may have happened weeks or months earlier. Food stock shortage. Malware could infect control systems, leading to the compromise of critical infrastructure such as irrigation systems or food processing plants. Compromised food safety. Attackers can tamper with or manipulate data related to food quality, contamination testing, or traceability, leading to the distribution of unsafe or adulterated food products. This can pose significant risks to public health, result in product recalls, and damage the	Ransomware Data breaches Supply Chain, Social engineering and phishing	IS & Network Lifecycle Security, OT security Supply Chain, Cloud Security Human resources, employees background checks Business Continuity & Supply Chain Security Crisis Management Cybersecurity awareness training

Specific NIS2 Other critical sectors impacts (Important Entities)	Industry specific threats or disruptions (pains)	Applicable NIS2 Risk management key measures & actions
reputation of food producers and suppliers. Disruption of the supply chain of the sector. Attacks targeting suppliers, distributors, or logistics providers can lead to delays in product delivery, shortages, or the introduction of counterfeit food products.		
Digital providers (search engines, marketplaces, social media platforms)	Search engine hijacking (changing user internet browser settings without user permission or awareness injecting false ads, pages links etc.) Advertisement links to malware, Search engine plug-in malware Social media fake accounts (seller, buyer) creation to fraud or spam, malware distribution or attack	ICT Lifecycle security Cybersecurity awareness training Incident management Supply Chain attacks
Manufacturing, production, distribution of chemicals Interruption in production Theft of recipes for fertilisers, Theft of materials, intermediate products,	Industrial cyberespionage Insider risks Social engineering & phishing Ransomware Data breaches OT/ICS cyber attacks	ICT Lifecycle security, OT security Encryption Physical Security
Research Selling data to competitors Theft of various intellectual property: recipes, patents, medical treatments leading to disruption or decrease of competitive advantage Physical theft inside or outside of the office R&D buildings of portable devices, paper documentation USB, SD cards, etc. where critical IP information is saved. Physical attacks theft related to R&D personnel.	Cyberespionage Selling data to competitors Physical theft, sabotage Social engineering & phishing	ICT Lifecycle security Encryption Physical security Human resources security, background checks Cybersecurity Awareness

Sources: Consolidated key information from cybersecurity landscape reports. Sources in Section 12.

7 Eviden’s approach to NIS2 compliance journey

In preparation for the NIS 2 Directive, organisations across various sectors are encouraged to undertake cybersecurity maturity assessments, risk assessments and compliance gap analyses to align with the new requirements. Then they intend to correct or adjust the documentation to be compliant and structured to easily find respective requirements being addressed in front of auditors. In addition, this proactive approach includes identifying and mitigating risks, implementing cybersecurity best practices, and ensuring effective incident response and recovery capabilities.

7.1 Holistic journey to join at any maturity or implementation stage

Eviden Team has developed holistic NIS2 Compliance Programme mapped to the newest NIST Cybersecurity Framework 2.0 functions: Govern, Identify, Protect, Detect, Respond, Recover grouped by independent NIS2 Domains.

After thorough analysis of NIS2 requirements, however, we rearranged them indicating on not integrated incident and crisis management or overlapping / repeating of several aspects (cyber hygiene with cyber awareness and zero trust repeating IS & network lifecycle security) within the list of NIS2 requirements called “risk management measures” addressed by Art. 21.2 a-j just to illustrate some of them.

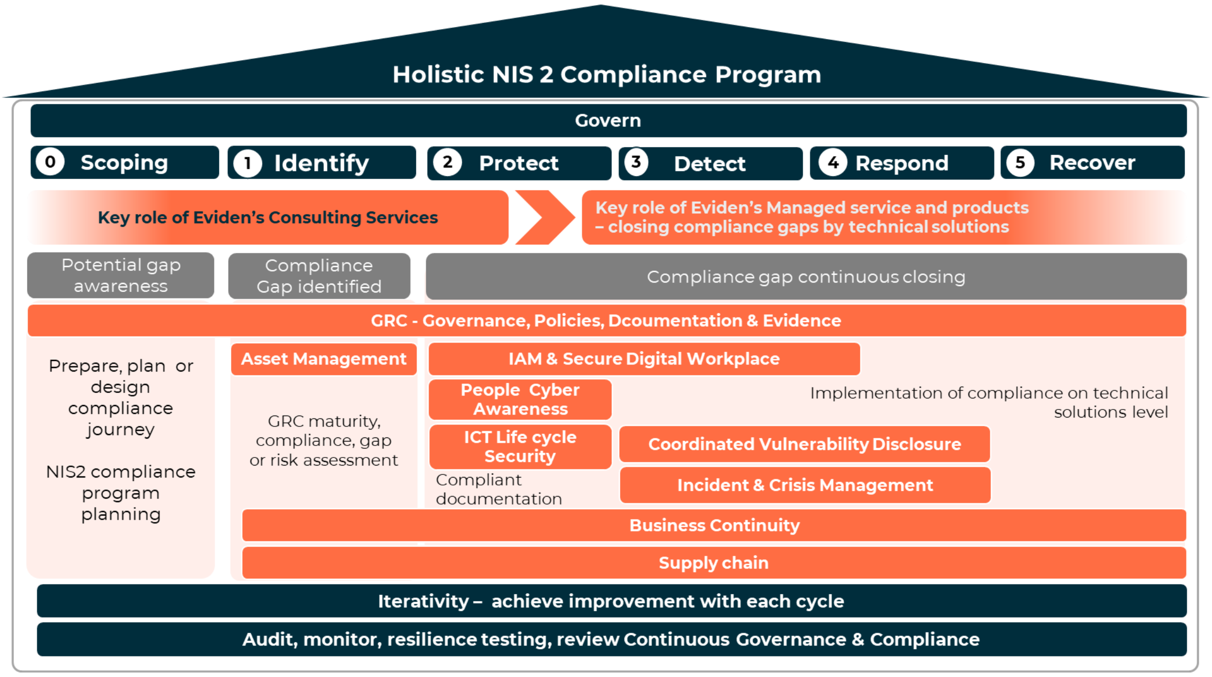
As a result of this grouping big domains emerged: GRC (grouped all NIS2 policies for: risk analysis, information security, cryptography, network & IS, access control), Incident & Crisis Management, Business Continuity, Supply Chain, ICT/OT Lifecycle security, People Cyber awareness and Background Checks, Asset Management, IAM, Secure Digital Workplace (under which Multifactor Authentication, Access control mechanisms, secure voice, emergency communication is contained).

Adding iterativity, monitoring, review, audit, resilience testing activity as part of integral element of the approach we integrate assurance into our approach.

Simultaneously, we mapped also typical programme management activities like proper scoping and program planning, from gap identification (GRC maturity, compliance gap or risk assessment), where key role plays here Eviden’s cybersecurity consulting service through meaningful recommendations, action plan, improvement planning and finally “closing the gap” activities – ending with execution of implementation plan by deploying products, managed security services to execute NIS2 on technical solutions compliance level or improving organisation’s documentation in a way that it is their contents, structure is aligned with NIS2 requirements and easily recognised as ‘compliant documentation’ by any regulatory auditor or supervisor.

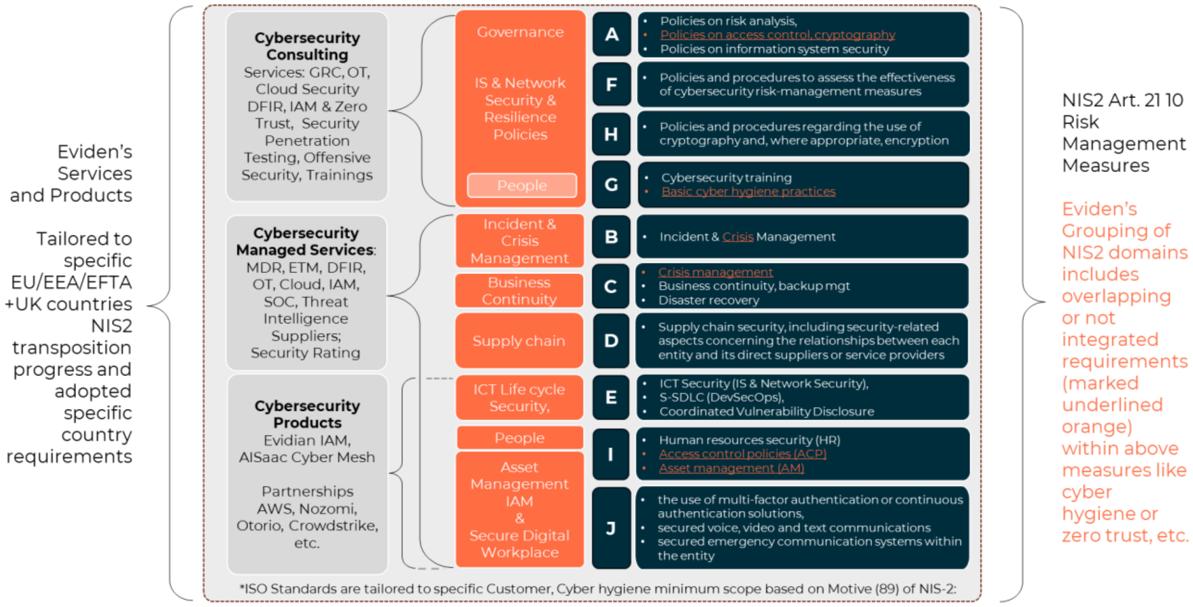
Eviden’s overall approach to NIS2 Compliance is depicted in Figure 15.

Figure 15 Eviden’s NIS2 Compliance Programme


Holistic NIS 2 Compliance Program
Govern
0 Scoping
1 Identify
2 Protect
3 Detect
4 Respond
5 Recover
Key role of Eviden’s Consulting Services
Key role of Eviden’s Managed service and products – closing compliance gaps by technical solutions
Potential gap awareness
Compliance Gap identified
Compliance gap continuous closing
GRC - Governance, Policies, Dcoumentation & Evidence
Prepare, plan or design compliance journey
NIS2 compliance program planning
Asset Management
GRC maturity, compliance, gap or risk assessment
IAM & Secure Digital Workplace
People Cyber Awareness
ICT Life cycle Security
Compliant documentation
Implementation of compliance on technical solutions level
Coordinated Vulnerability Disclosure
Incident & Crisis Management
Business Continuity
Supply chain
Iterativity – achieve improvement with each cycle
Audit, monitor, resilience testing, review Continuous Governance & Compliance

Source: Eviden’s own elaboration. All rights reserved.

Figure 16 Eviden NIS2 domains grouping


Eviden’s Services and Products
Tailored to specific EU/EEA/EFTA +UK countries NIS2 transposition progress and adopted specific country requirements
Cybersecurity Consulting
Services: GRC, OT, Cloud Security DFIR, IAM & Zero Trust, Security Penetration Testing, Offensive Security, Trainings
Cybersecurity Managed Services: MDR, ETM, DFIR, OT, Cloud, IAM, SOC, Threat Intelligence Suppliers; Security Rating
Cybersecurity Products
Evidian IAM, AISaac Cyber Mesh
Partnerships AWS, Nozomi, Otorio, Crowdstrike, etc.
Governance
IS & Network Security & Resilience Policies
People
Incident & Crisis Management
Business Continuity
Supply chain
ICT Life cycle Security,
People
Asset Management IAM & Secure Digital Workplace
A
Policies on risk analysis,
Policies on access control, cryptography
Policies on information system security
F
Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
H
Policies and procedures regarding the use of cryptography and, where appropriate, encryption
G
Cybersecurity training
Basic cyber hygiene practices
B
Incident & Crisis Management
C
Crisis management
Business continuity, backup mgt
Disaster recovery
D
Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
E
ICT Security (IS & Network Security),
S-SDLC (DevSecOps),
Coordinated Vulnerability Disclosure
I
Human resources security (HR)
Access control policies (ACP)
Asset management (AM)
J
the use of multi-factor authentication or continuous authentication solutions,
secured voice, video and text communications
secured emergency communication systems within the entity
*ISO Standards are tailored to specific Customer, Cyber hygiene minimum scope based on Motive (89) of NIS-2:
NIS2 Art. 21 10 Risk Management Measures
Eviden’s Grouping of NIS2 domains includes overlapping or not integrated requirements (marked underlined orange) within above measures like cyber hygiene or zero trust, etc.

Source: Eviden’s own elaboration.

7.2 Complete NIS2 mapping to multiple industry or MS standards

Eviden’s Team is formulating the thesis that EU regulations can be mapped to multiple cybersecurity or cyber resilience best practices as they are already covering the whole scope of NIS2 requirements by various ISO, ISA, NIST, ITU-T, ENISA and other standards developed by renowned institutions, associations, or other organizations.

Also, in some of the industries it is possible to map specific standard which are currently used by organisations to be recognised as addressing certain extent of NIS2 requirements coverage. This could include specific ISMS (Information Security Management Systems) for industries like ISO/IEC 27019 for energy, or TISAX for automotive industry or even country specific ISMS like the one in Germany BSI requirements.

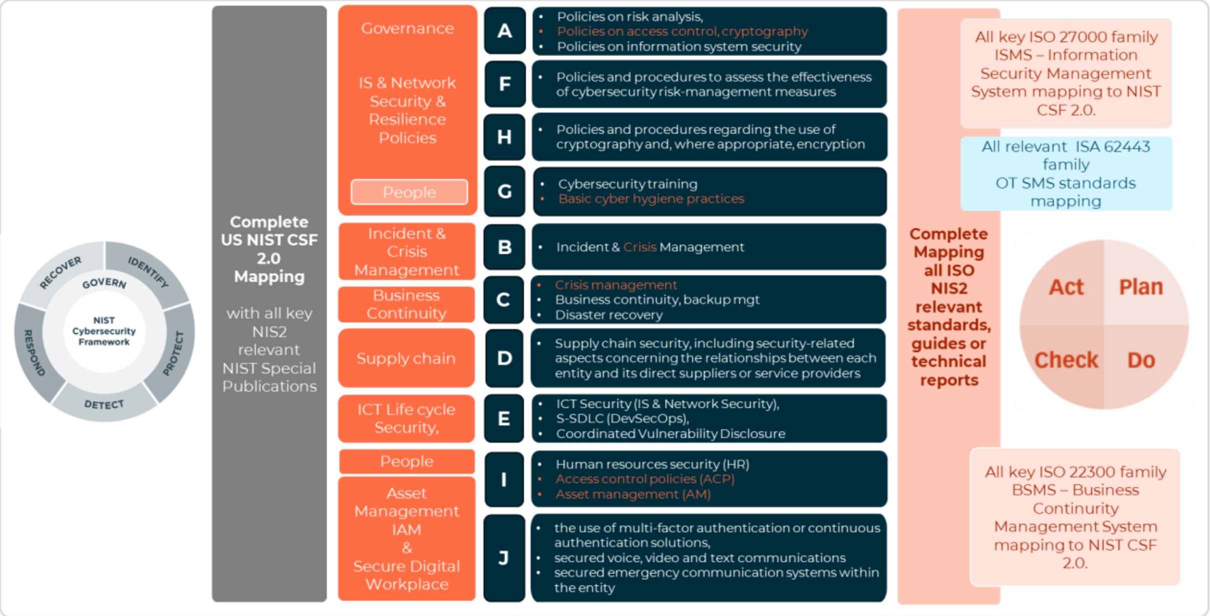
With each engagement Eviden's Team brings to our customers overview of existing standards package and share how to optimally address various best practices to respond to NIS2 requirements with EU regulatory "proportionality principle".

Despite variety of available standard there existing key standards determining management of cybersecurity domain in each organisation, which can be described as ISMS – Information Security Management System with ISO/IEC 27001:2022 standard or as CSF – Cybersecurity Framework with NIST CSF 2.0 version. These standards are point of start for addressing NIS2 requirements in the domain of information security or its subdomain – cybersecurity. However, NIS2 requirements are going beyond information security itself as also cyber resilience aspect is addressed. Therefore, such standards as ISO/IEC 22301 addressing BCMS - Business Continuity Management System or ISO/IEC 28000 are referenced to address supply chain security.

With abundance of best practices, it is easily to lose integrated picture of NIS2 requirements which needs to be managed to satisfy NIS2 compliance. Eviden's Team on continuous basis is monitoring progress in best practices addressing scope of EU-wide and worldwide cybersecurity or information security regulations. We analyse dependencies between them to create integrated, holistic frameworks of requirements to make sure Eviden's customers have the most up-to-date advice regarding how to utilise best thought leadership and experience to reasonably practicable, efficiently, and proportionally answer to NIS2 compliance challenges.

For which if the domain standards we have already prepared more detailed references to 100+ specific standards which might be appliable whether for the specific industry, subsector of NIS2, region or country, anticipating the need of compliance also non-EU originated organisation performing business activities on EU (for example for UK, Eviden Team may address mapping between UK Cybersecurity Assurance Framework, ISO 27001, ISO 22301 with NIS2 requirements. High level summary of main families of standards are highlighted on Figure 17. Please contact Eviden Team for in case of need for specific engagement.

Figure 17 Eviden's NIS2 approach contains mapping to all NIS2 relevant industry standards


RECOVER
IDENTIFY
GOVERN
NIST Cybersecurity Framework
RESPOND
PROTECT
DETECT
Complete US NIST CSF 2.0 Mapping
with all key NIS2 relevant NIST Special Publications
Governance
IS & Network Security & Resilience Policies
People
Incident & Crisis Management
Business Continuity
Supply chain
ICT Life cycle Security,
People
Asset Management IAM & Secure Digital Workplace
A
• Policies on risk analysis,
• Policies on access control, cryptography
• Policies on information system security
F
• Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
H
• Policies and procedures regarding the use of cryptography and, where appropriate, encryption
G
• Cybersecurity training
• Basic cyber hygiene practices
B
• Incident & Crisis Management
C
• Crisis management
• Business continuity, backup mgt
• Disaster recovery
D
• Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
E
• ICT Security (IS & Network Security),
• S-SDLC (DevSecOps),
• Coordinated Vulnerability Disclosure
I
• Human resources security (HR)
• Access control policies (ACP)
• Asset management (AM)
J
• the use of multi-factor authentication or continuous authentication solutions,
• secured voice, video and text communications
• secured emergency communication systems within the entity
Complete Mapping all ISO NIS2 relevant standards, guides or technical reports
All key ISO 27000 family ISMS – Information Security Management System mapping to NIST CSF 2.0.
All relevant ISA 62443 family OT SMS standards mapping
Act
Plan
Check
Do
All key ISO 22300 family BSMS – Business Continuirty Management System mapping to NIST CSF 2.0.

Source: Eviden's own elaboration.

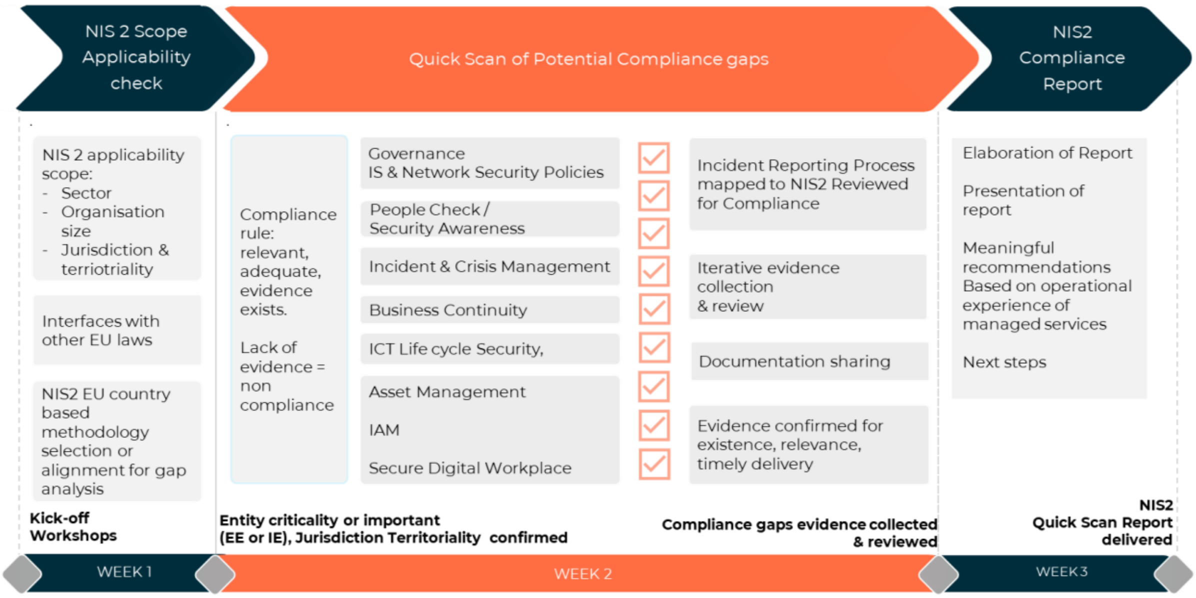
7.3 Key cybersecurity consulting offerings

7.3.1 Compliance gap quick scan

Eviden’s quick scan high-level compliance gap assessment focuses on the identification of the gap with remarks, (excluded analysis of impact of compliance and related business and audit material issue risk to the identified compliance gaps, and risk mitigations – all of exclusions are part of offer #4). This service addressed to organisation who aim to quick NIS2 gaps diagnosis without entering risk impacts and details, which seek for compliance checklist and action plan rather than addressing also risk scenarios related to identified compliance gaps. Quick scan is also perfect service for smaller organisations which do not have internal competencies to perform analysis or want to gradually engage in compliance journey.

Quick scan is conducted in the following steps as shown on the diagram below. Based on agreed checklist form, compliance gap assessment is performed using Eviden’s evidence-based approach (see Section 407.3.4).

Diagram 1 Compliance Gap Quick Scan



NIS 2 Scope Applicability check

Quick Scan of Potential Compliance gaps

NIS2 Compliance Report

NIS 2 applicability scope:
- Sector
- Organisation size
- Jurisdiction & terriotriality

Interfaces with other EU laws

NIS2 EU country based methodology selection or alignment for gap analysis

Kick-off Workshops

Compliance rule: relevant, adequate, evidence exists.

Lack of evidence = non compliance

Governance IS & Network Security Policies

People Check / Security Awareness

Incident & Crisis Management

Business Continuity

ICT Life cycle Security,

Asset Management

IAM

Secure Digital Workplace

Incident Reporting Process mapped to NIS2 Reviewed for Compliance

Iterative evidence collection & review

Documentation sharing

Evidence confirmed for existence, relevance, timely delivery

Entity criticality or important (EE or IE), Jurisdiction Territoriality confirmed

Compliance gaps evidence collected & reviewed

Elaboration of Report

Presentation of report

Meaningful recommendations Based on operational experience of managed services

Next steps

NIS2 Quick Scan Report delivered

WEEK 1

WEEK 2

WEEK 3

Source: Eviden’s own elaboration. All rights reserved.

7.3.2 Comprehensive risk-based compliance assessment (deep-dive)

In case organisations are using enterprise-wide risk management system (ERM COSO or ISO 31000, etc.) or performing already risk assessment or risk treatment based on requirements of certified ISO management systems standards or which (organisations) decided to use risk-based compliance assessment service as complementary deep-dive risk analysis of compliance with NIS2 Directive then this Eviden’s deep dive advisory service is perfect fit for them as results of this assessment are communicated by risk level. Moreover, this service addresses prioritisation of identified gap based on risk they pose to the organisation’s cyber resilience related risks. Optionally this deep dive assessment includes risk trade-off compliance assurance cost vs business and regulatory risk by connecting the dots between them.

Risk-based compliance assessment is for organization in scope of NIS2 which have internal certain competences on risk assessment and available employees to cooperate with Eviden consultant, or which have defined internal processes of enterprise risk management or similar ones.

Note: Risk-based compliance gap assessment can be complete (holistic) for all or per specific NIS-2 security countermeasures (art. 21.2.a to j) or combined in groups as mutually agreed with clients). Each group of NIS2 requirements are domains with broad subject matter scope, therefore some organisations may perceive or focus on the NIS2 aspect which they perceive as highest risk or most critical for their business mission. Also, such organisation may want to have independent view on specific domain to challenge current perception of it their organisation.

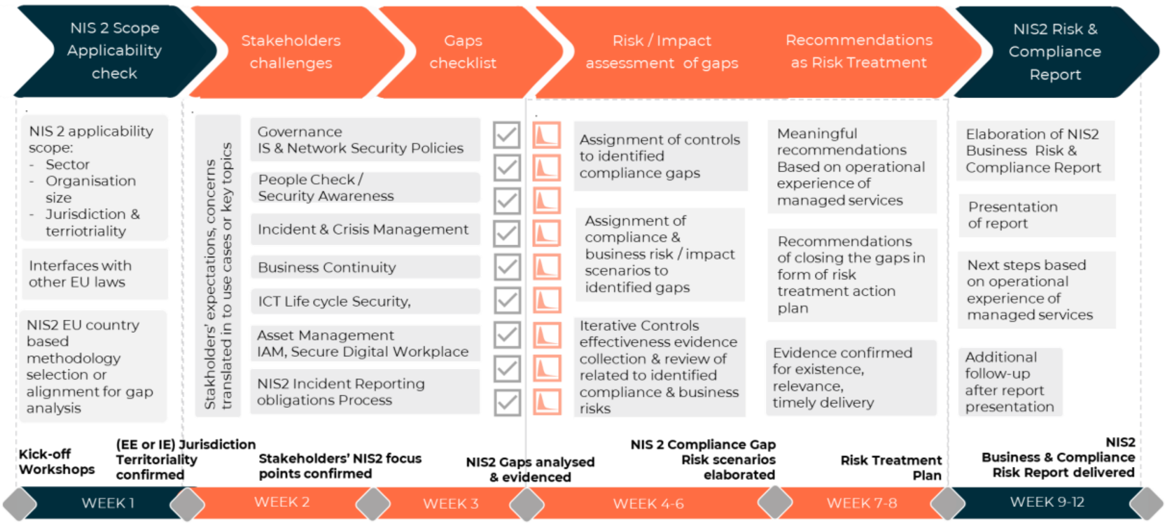
Risk-based compliance assessment is composed of the following phases:

1. **NIS2 scope applicability check**

   In this phase, the regulations applicable to specific services are discussed with organisation's head legal or compliance unit in detail to determine to which entity class NIS2: essential or important entity - will potentially be assigned. We are assisting, if necessary, in consultations of organisation's specific question, cases with the specific EU member state regulator.

   Deliverable: This results in the confirmation and assignment of analysed organisation to essential or important entity class and territoriality and jurisdiction applicability, especially in the situations where analysed company conducts its business activities in more than one EU Member State. It also may include (dependent on agreement) interfaces with related EU Regulations like DORA or CER as it could happen that bigger capital groups may fall, apart from NIS2 requirements into DORA requirements as Third-Party Service Provider (i.e., big telecommunication or energy sector group which serves its business-to-business services to financial institutions.

Diagram 2 Risk-based compliance assessment


NIS 2 Scope Applicability check
Stakeholders challenges
Gaps checklist
Risk / Impact assessment of gaps
Recommendations as Risk Treatment
NIS2 Risk & Compliance Report
NIS 2 applicability scope:
- Sector
- Organisation size
- Jurisdiction & terriotriality
Interfaces with other EU laws
NIS2 EU country based methodology selection or alignment for gap analysis
Stakholders' expectations, concerns translated in to use cases or key topics
Governance IS & Network Security Policies
People Check / Security Awareness
Incident & Crisis Management
Business Continuity
ICT Life cycle Security,
Asset Management IAM, Secure Digital Workplace
NIS2 Incident Reporting obligations Process
Assignment of controls to identified compliance gaps
Assignment of compliance & business risk / impact scenarios to identified gaps
Iterative Controls effectiveness evidence collection & review of related to identified compliance & business risks
Meaningful recommendations Based on operational experience of managed services
Recommendations of closing the gaps in form of risk treatment action plan
Evidence confirmed for existence, relevance, timely delivery
Elaboration of NIS2 Business Risk & Compliance Report
Presentation of report
Next steps based on operational experience of managed services
Additional follow-up after report presentation
Kick-off Workshops
(EE or IE) Jurisdiction Territoriality confirmed
Stakeholders' NIS2 focus points confirmed
NIS2 Gaps analysed & evidenced
NIS 2 Compliance Gap Risk scenarios elaborated
Risk Treatment Plan
NIS2 Business & Compliance Risk Report delivered
WEEK 1
WEEK 2
WEEK 3
WEEK 4-6
WEEK 7-8
WEEK 9-12

Source: Eviden's own elaboration. All rights reserved.

2. **NIS2 internal stakeholder's expectations, concerns, challenges, priorities, end-result**

   a. NIS2 compliance gap assessment is not only CISO job, therefore at least the following stakeholders should be consulted on their priorities, expectations, etc.:
      i. Executive Board (C-Level is mentioned in NIS2 as "management bodies" individually responsible for NIS2 compliance of the organisation they manage).
      ii. CISO/CIO/BCM/Crisis Management/COO Stakeholders – responsible directly for cybersecurity and operational resilience controls, planning & execution.
      iii. Head of Compliance and/or Legal Department.
      iv. Key suppliers (subcontractors) if their impact affects the continuity or resilience of services performed for organisation's retail, wholesale / B2B clients.
      v. Any other internal or external stakeholder which should be considered to consult in specific situations. This is usually clarified at the beginning of the engagement during kick-off and stakeholder's workshops)

b. Optionally (if relevant) NIS2 Awareness Training could be conducted to all key internal stakeholders, who influence or affect NIS2 compliance activities and accountability to the Regulator, and regulatory sanctions.

   Deliverable: All the expectations, end-results to be achieved, requirements, concerns, priorities, challenges are documented and recorded for next phases.

3. **Gap checklist adoption or elaboration, execution of compliance gap assessment**.

   This is the phase where compliance gap checklists and high-level risk / impact scenarios are defined based on the deliverable(s) obtained from the previous phase – i.e. documented stakeholders needs, expectations, requirements, priorities, result, etc. In specific situation potential customer could address that in some of the domains more specific or granular checklist will be elaborated or adopted based on customer input on cyber risks (if such report exists).

   Next, also it is agreed if compliance gap checklist would refer to controls / safeguards from ISO, ISA, NIST standards or for example to deliverables required. This granularity level for checklist may differ from organisation to organisation as the one may already operate within ISO certified management system like ISMS (ISO 27001 information security), BCMS (ISO 22301 business continuity), IT SMS (ISO 20000 IT Service Management) or SC SMS (ISO 28000 – Supply Chain Security Management System) or the other ones.

   At this stage checklist is also adopted to stakeholder's objectives expressed in the previous phase. Specific scope of checklist and NIS gaps identification may refer to preparation of recommendations on how to close potentially discovered gaps to demonstrate compliance status quo in front of B2B Client including evidence collection & review process which first must be implement internally and then such process should deliver respective summary for analysed organisation's clients.

   Finally based on agreed checklist form, compliance gap assessment is performed using Eviden's evidence-based approach (see Section 407.3.4).

   Deliverables:

   - Compliance gap assessment checklist elaborated including organisation internal and external context.

   - Compliance gap assessment execution

4. **Performing Risk-based compliance assessment**

   Based on compliance gap assessment performed in the previous phase, formally agreed list of risk scenarios (as agreed in the bidding phase) is to be assigned to given identified compliance gaps and referring organisation risk acceptance level, tolerances, limits with reference to NIS2 article or group of articles (if justified in terms of synergy).

   Deliverables: assessment of risks related to identified NIS2 compliance and mapping them to organisations acceptable risk level, tolerances, or limits.

5. **Recommendations – identification of missing controls, improvement actions to achieve NIS2 compliance status and supporting evidence.**

   At this stage meaningful, executable recommendations are drawn up on how to close identified potential compliance gaps and what risk treatment activities related to risk assigned to specific gap should implemented. At that stage, the client is consulted on their adequacy, proportionality rule, relevancy and priority and justification for their implementation. This service does not include closing the gap or risk treatment activities implementation as it is part & scope of separate Eviden's consulting service.

Deliverable: recommendations on optimal way to close NIS2 compliance gap and related risk treatment plan addressing compliance or business risk scenarios.

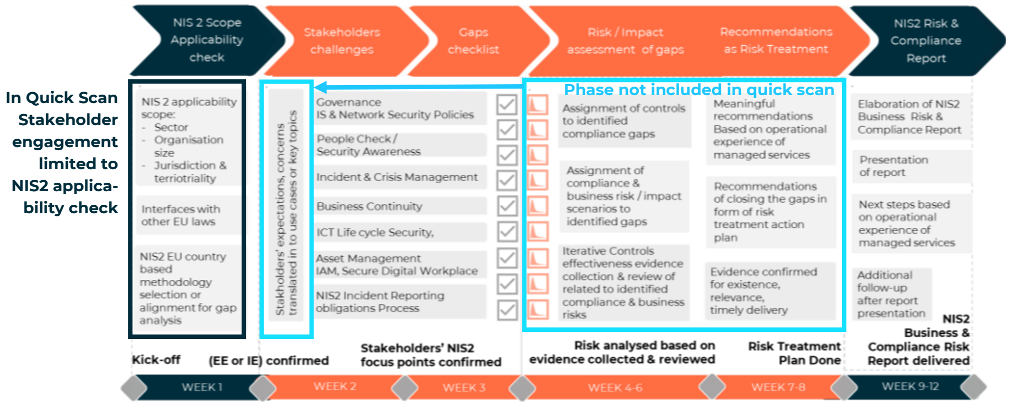
6. **Presentation of NIS2 Risk-based Compliance Gap Assessment Report**

   At this stage final NIS2 risk & compliance report is drawn up and consulted (up to number of agreed interactions - sent for approval, review, correction, or adaptation and then given for final approval). Presentation of the identified results of the report and possible next steps. Project ends.

   Deliverable: NIS2 Risk Scenarios & Compliance Gap Assessment Report

Based on the above high-level risk-based compliance assessment service description the difference between quick scan and risk-based assessment are as shown in Figure 18.

Figure 18 Differences between NIS2 2risk-based compliance assessments and quick scans.



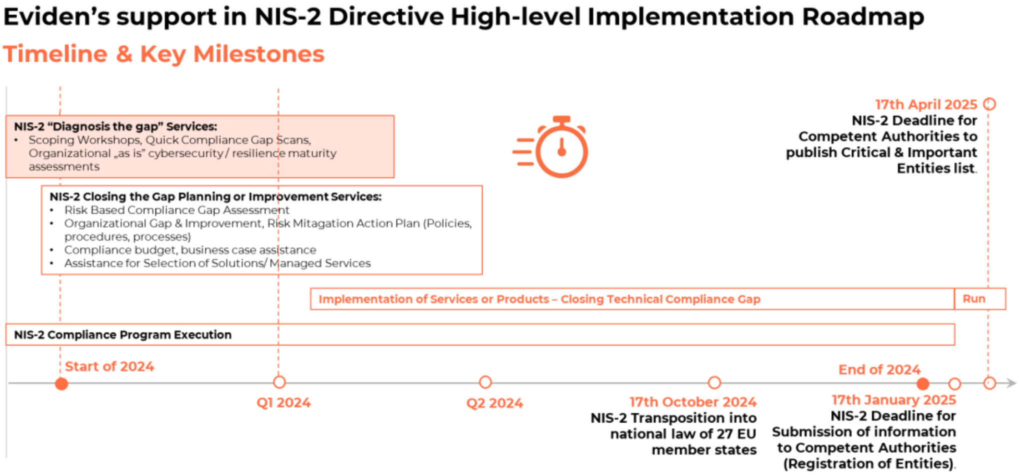
NIS 2 Scope Applicability check
Stakeholders challenges
Gaps checklist
Risk / Impact assessment of gaps
Recommendations as Risk Treatment
NIS2 Risk & Compliance Report
In Quick Scan Stakeholder engagement limited to NIS2 applicability check
NIS 2 applicability scope: - Sector - Organisation size - Jurisdiction & terriotriality
Interfaces with other EU laws
NIS2 EU country based methodology selection or alignment for gap analysis
Stakeholders' expectations, concerns translated in to use cases or key topics
Governance IS & Network Security Policies
People Check / Security Awareness
Incident & Crisis Management
Business Continuity
ICT Life cycle Security,
Asset Management IAM, Secure Digital Workplace
NIS2 Incident Reporting obligations Process
Phase not included in quick scan
Assignment of controls to identified compliance gaps
Assignment of compliance & business risk / impact scenarios to identified gaps
Iterative Controls effectiveness evidence collection & review of related to identified compliance & business risks
Meaningful recommendations Based on operational experience of managed services
Recommendations of closing the gaps in form of risk treatment action plan
Evidence confirmed for existence, relevance, timely delivery
Elaboration of NIS2 Business Risk & Compliance Report
Presentation of report
Next steps based on operational experience of managed services
Additional follow-up after report presentation
Kick-off
(EE or IE) confirmed
Stakeholders' NIS2 focus points confirmed
Risk analysed based on evidence collected & reviewed
Risk Treatment Plan Done
NIS2 Business & Compliance Risk Report delivered
WEEK 1
WEEK 2
WEEK 3
WEEK 4-6
WEEK 7-8
WEEK 9-12

Source: Eviden's own elaboration. All rights reserved.

7.3.3 Other cybersecurity NIS2 priority service packages

Below there are characterised key Eviden's services packages and how they can support NIS2 implementation roadmap. Services with number #1 to #4 are called quick diagnosis consulting services and services with number #5 to #7 are called closing the gap consulting services. Services #8 and #9 are Program or project management services related to implementation of compliance program or dedicated to implementation of specific managed security services available in Eviden's portfolio described in Section 7.4

Figure 19 Eviden's NIS2 Compliance Implementation Roadmap



Eviden's support in NIS-2 Directive High-level Implementation Roadmap
Timeline & Key Milestones
NIS-2 "Diagnosis the gap" Services:
• Scoping Workshops, Quick Compliance Gap Scans, Organizational „as is" cybersecurity / resilience maturity assessments
NIS-2 Closing the Gap Planning or Improvement Services:
• Risk Based Compliance Gap Assessment
• Organizational Gap & Improvement, Risk Mitagation Action Plan (Policies, procedures, processes)
• Compliance budget, business case assistance
• Assistance for Selection of Solutions/ Managed Services
Implementation of Services or Products – Closing Technical Compliance Gap
Run
NIS-2 Compliance Program Execution
17th April 2025
NIS-2 Deadline for Competent Authorities to publish Critical & Important Entities list.
Start of 2024
Q1 2024
Q2 2024
17th October 2024
NIS-2 Transposition into national law of 27 EU member states
End of 2024
17th January 2025
NIS-2 Deadline for Submission of information to Competent Authorities (Registration of Entities).

Source: Eviden's own elaboration.

Table 9 Specific NIS2 Consulting Service packages and program management

No.	NIS2 Service Packages (SP)	Description	High-Level Duration
#1	Cybersecurity Maturity Level (COBIT, C2M2, NIST CSF, etc.)	Assessment aiming at determination as is level	2-4 weeks dependent on customer maturity level and organization size, and other specific parameters
#2	EU-Regulations Compliance Scoping Workshop (especially for bigger companies with many international locations)	Checking applicability scope for specific regulations or combined regulatory requirements like DORA-CER or NIS-2 CER, or any other overlap with industry specific regulations, etc.	1-2 weeks dependent on customer maturity level and organization size, and other specific parameters
#3	EU-Regulations Quick Compliance Scan Gap	Quick high-level compliance gap assessment (identification of the gap with remarks, (excluded analysis of impact of compliance and related business and audit material issue risk to the identified compliance gaps, and risk mitigations – all of exclusions are part of offer #4)	1-2 weeks dependent on customer maturity level and organization size, and other specific parameters
#4	EU-Regulations Risk Based Compliance Gap Assessment with meaningful recommendations and action plan.	Deep dive compliance gap assessment with risk tradeoff compliance assurance cost vs business and regulatory risk Note: Compliance gap assessment can be complete (holistic) or per specific NIS-2 security countermeasures (art. 21.2.a to j) or DORA Pillar 1 to 5 or combined in groups as mutually agreed with clients)	7-12 weeks dependent on customer maturity level and organization size, and other specific parameters (like number of locations)
#5	Organizational compliance gap improvement / transformation plan – elaboration of detailed plan	Closing Compliance gap through governance, policies, procedures, evidence collection and documentation adjustment,	4-6 weeks dependent on customer data availability and quality of data.

No.	NIS2 Service Packages (SP)	Description	High-Level Duration
		improvement, etc. (this service delivers high quality content procedures, policies but excludes approval process according to customer internal procedures which is supposed to be done by customer)	
#6	Compliance budget, business case assistance, management buy-in	Elaboration of business case for specific regulatory gap or gaps combined into one business case	2-4+ weeks dependent on customer data availability and quality of data and number of business cases defined in scope
#7	RFI/RFP Assistance for Selection of Solutions, Managed Services for closing the compliance gap	Elaboration of specific RFI/RFP addressing specific compliance gap or combined gaps into one RFI/RFP (this service includes subject matter input to RFP, excluding formatting, commercial information gathering, etc.)	1-4 weeks dependent on the size of RFI/RFP
#8	Technical, architectural compliance gap improvement / transformation plan or onboarding of managed services (see separate slide)	Elaboration of architectural changes, infrastructure, cloud migration for specific regulatory gap or gaps combined into one business case	4-12+ weeks dependent on customer data availability and quality of data and number of specific architectural designs necessary
#9	Execution of compliance program or implementation project or coordination of non-project activities.	Execution, Management of specific Regulatory Compliance Program of project.	Dependent on project schedule.

Source: Eviden's own elaboration.

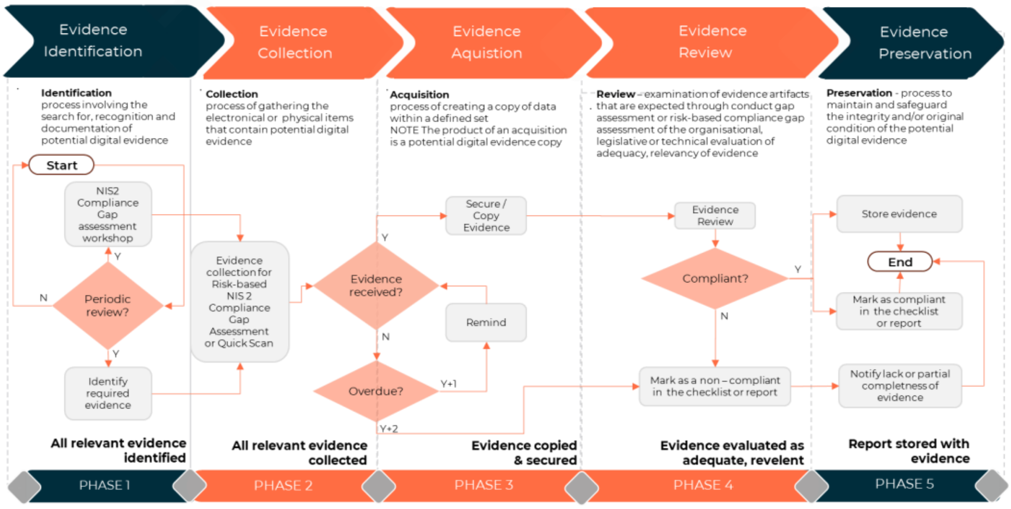
7.3.4 Evidence-based NIS2 Compliance Assessment

All Eviden's Consulting services are performed with evidence-based approach aligned with ISO/IEC 27037:2012 Standard: 'Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.' Review phase is added by Eviden team to follow the process of advisory services here.

Why Eviden's Team endorses evidence-based assessment? In particular to demonstrate both compliance whether ex ante or ex post regulatory audit or during reporting obligations under art. 23 of

NIS2 we are of the opinion that without proper ownership and establishment of evidence collection and review process, procedure organisations in scope of NIS2 will not be able to justify actions taken, or prove that prevention measures were adequate, proportional and up to date to state-of-the-art.

Diagram 3 Evidence collection process for NIS2 Compliance Assessment Services


Evidence Identification
Evidence Collection
Evidence Aquistion
Evidence Review
Evidence Preservation
Identification process involving the search for, recognition and documentation of potential digital evidence
Collection process of gathering the electronical or physical items that contain potential digital evidence
Acquisition process of creating a copy of data within a defined set NOTE The product of an acquisition is a potential digital evidence copy
Review – examination of evidence artifacts that are expected through conduct gap assessment or risk-based compliance gap assessment of the organisational, legislative or technical evaluation of adequacy, relevancy of evidence
Preservation - process to maintain and safeguard the integrity and/or original condition of the potential digital evidence
Start
NIS2 Compliance Gap assessment workshop
Y
N
Periodic review?
Y
Identify required evidence
Evidence collection for Risk-based NIS 2 Compliance Gap Assessment or Quick Scan
Evidence received?
Y
N
Secure / Copy Evidence
Remind
Overdue?
Y+1
Y+2
Evidence Review
Compliant?
Y
N
Mark as a non – compliant in the checklist or report
Store evidence
End
Mark as compliant in the checklist or report
Notify lack or partial completness of evidence
All relevant evidence identified
All relevant evidence collected
Evidence copied & secured
Evidence evaluated as adequate, revelent
Report stored with evidence
PHASE 1
PHASE 2
PHASE 3
PHASE 4
PHASE 5

Source: Eviden's own elaboration. Definitions come from ISO 27037:2012 standard.

In specific applications this evidence-based assessment process may differ from customer to customer being in scope of NIS2. Evident Team will use proportionality rule to address organisation size, broadness, and complexity of ICT environments of the specific entities, whether essential or important.

7.4 Eviden's NIS2 Cybersecurity services and products portfolio

Table 10 Closing NIS2 Compliance Gap with Eviden's Cybersecurity Services or Products

NIS-2 Article 21.2	Eviden's Cyber Security Services (CyS) with Partner's products supporting the service	Eviden's / Partners' Cybersecurity Products
(a) Policies on risk analysis and information system security	GRC Consulting, Risk Assessment, Security Compliance CYS Cyber Security Integration	Eviden Partners' Products
(b) Incident handling.	Cybersecurity Consulting: DFIR, GRC CYS DFIR Managed Services, CSIRT CYS Managed Security Operations, Sec Consult: Incident Response CYS Managed Detection & Response CYS Cyber Security Integration	Eviden Partners' Products Eviden's AIsaac Cyber Mesh
(c) Business continuity, disaster recovery and crisis management.	GRC Consulting Sec Consult: Incident Response CYS DFIR Managed Services, CSIRT CYS Cyber Security Integration	Eviden Partners' Products
(d) Supply-chain security, including security-related aspects concerning the relationships between each entity and its suppliers or service providers.	Cybersecurity Consulting: up to all of Practices, in particular GRC, Penetration Testing, Sec Consult: Red Teaming Service CYS Cloud and Application Security, CYS DFIR Managed Services: Suppliers Security Rating CYS OT/IoT CYS OT/IoT Security Services	CYP IAM Products - Evidian Eviden's AIsaac Cyber Mesh

NIS-2 Article 21.2	Eviden's Cyber Security Services (CyS) with Partner's products supporting the service	Eviden's / Partners' Cybersecurity Products
	CYS Cyber Security Integration CYS OT Security Integration	
(e) Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure	CYS DFIR Managed Services: Vulnerability Management Service, CYS Managed Security Operations, CYS OT/IoT CYS OT/IoT Security Services CYS OT Security Integration	Eviden Partners' Products Eviden's AIsaac Cyber Mesh
(f) Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.	CYS DFIR Managed Services: Threat Intelligence/Hunting as part of TLTP, Vulnerability Management Service, EASM Cybersecurity Consulting: Penetration Testing, Sec Consult: Red Teaming Service CYS Managed Security Operations, Sec Consult: Red Teaming Service	Eviden Partners' Products Eviden's AIsaac Cyber Mesh
(g) Cyber hygiene* practices and cybersecurity training.	All relevant Eviden Portfolio of Managed Services, Products – dependent on customer definition or applicability scope of „cyber hygiene" CYS Security Training and Awareness	Eviden Partners' Products
(h) Policies on the use of cryptography and encryption.	GRC Consulting: Digital Sovereignty Advisory	CYP Crypto Products (Trustway) - Data Protection solutions (Trustway DataProtect), HSM - Hardware Security Modules (Trustway Proteccio), Network encryption (Trustway IP Protect), Payment & IoT HSM CYP Digital ID (Cryptovision) - Cryptovision SCinterface VSC, Cryptovision SCinterface, Cryptovision SCinterface Cache, GreenShield Product Sheet, Cryptovision ePasslet Suite Technical Data Sheet, CardOS versions overview, Secure citizen-centric Digital Identity Solutions Eviden Partners' Products

Source: Eviden's own elaboration

*Cyber hygiene minimum scope based on Motive (89) of NIS-2:

- zero-trust principles,
- software updates,
- device configuration,
- network segmentation,
- identity and access management or user awareness,
- security awareness training of staff on cyber threats, phishing, or social engineering techniques)

For further information, please consult Eviden's Team who will guide you with cybersecurity experts or legal advisors to ensure comprehensive NIS2 compliance.

7.5 Customer success stories – NIS2 Compliance Eviden Projects

Everything what has been based written in this whitepaper comes from Eviden's practical hands-on experience from Cybersecurity Governance Risk Compliance customer engagement and from completed or ongoing NIS2 consulting or managed services projects. Exemplary engagements on NIS2 include among others:

1. Manufacturing Packaging company in Netherlands.
2. One of biggest fund in Switzerland – where NIS2 was one of broader compliance consultancy project next to DORA, CRA and Cyber suppliers' assurance framework.
3. Chemical Company in Austria
4. Capital city of one of EU Member States.
5. Brewery Company in Austria
6. Energy & Steel Manufacturing Company in Austria
7. Telecommunication & Broadcasting Regulator in one of EU Member States
8. Research & Development sector company in Belgium
9. Food (Cheese) Manufacturing Company in Germany
10. Manufacturing of Plastics in Austria.
11. Public Administration - Governmental Ministry of Transportation of one of EU Member States.

8 Closing remarks, next streps and further assistance

We ended being your companion to NIS2 Compliance Journey. Natural questions arise on what to do next. How to turn into action the knowledge acquired with this whitepaper?

Key takeaways we would like to underline can be listed as follows:

- Elaborate or review your ISMS in view of ISO 27001/2 Controls, and ISO 22301 controls, CIS Controls & applicable Benchmarks, NIST Cybersecurity Framework or other applicable Cybersecurity Framework – what is preferable way of communication of cybersecurity processes maturity level under NIS 2 Directive
- Check your current Country security standards and security measures defined for NIS 1 already and monitor progress of adoption (transposition) of NIS 2 to your country cybersecurity system.
- Elaborate or review your current cybersecurity risk assessment process or framework, cybersecurity measurement approach (measure what matters) if it generates respective information for risk-based decision making or acceptance.
- Elaborate or review your business continuity process and cyber recovery processes.
- Document your Incident handling process if it can satisfy NIS 2 reporting time limits for incidents.
- Assess your Supply Chain Cybersecurity Risk
- Create a Vulnerability Disclosure Policy. Put procedures in place to receive vulnerability notifications from third parties.
- Promote and implement DevSecOps.
- If your company is under NIS 1 focus on compliance gaps which result from transition to NIS 2 and check again applicability.

- Check if your organization is in scope of NIS 2 – and if yes to which of two groups of entities it will be classified:
    - Essential Sectors/Industries Entities (see detailed information separate slide)
    - Important Sectors/Industries Entities ((see detailed information separate slide)
    - Make aware your management board about its obligations, it is not CISO exercise, above all it is board member responsibility (CISO is not mentioned at all in NIS 2 Directive) on the requirements & penalties of NIS 2, in particular Board Member responsible for cybersecurity and resilience (BCM Program), could be CEO or Chief Operating Officer) and also Chief Compliance Officer, Chief Risk Officer.
- Select the ISMS or Cybersecurity framework which best fits to your organization's industry, region, clients, company size, partners, regulator, etc. – based on 10 cybersecurity management measures in Article 21
- Based on selected appropriate Cybersecurity Framework – perform risk-based compliance gaps self-assessment starting with review of IT- OT asset management process & inventory review - with independent party, remembering that NIS2 requires IT and OT being managed integrally – including key security processes required for compliance with NIS2
- Present to Executives - NIS2 Risk Based Compliance Gaps Report and prioritize them for remediation.
- Based on specific business cases involve management to plan budget for eventual compliance gap remediation project.
- Elaborate or review existing cybersecurity training and make sure it is documented. NIS 2 mandates regular training and risk ownership for all executives.
- Make sure that remediation has taken place and there is a plan for periodic review or penetration testing of existing IT & OT controls.

These are of course exemplary actions. The Eviden Team is ready to assist you in your journey regardless of the stage you are at or cybersecurity maturity of your organization. Contact us and we will respond.

9 About Eviden

9.1 Consulting capability

We foster collaborative relationships with CISOs, encouraging open communication and effective strategy development. We speak the language of Board of Directors, CxO being able to communicate with any level of the organisation. We build strong partnerships with key cybersecurity stakeholders in the organization to unlock the power of open communication and drive effective security strategy development even if we are not currently engaged in projects with specific customers.

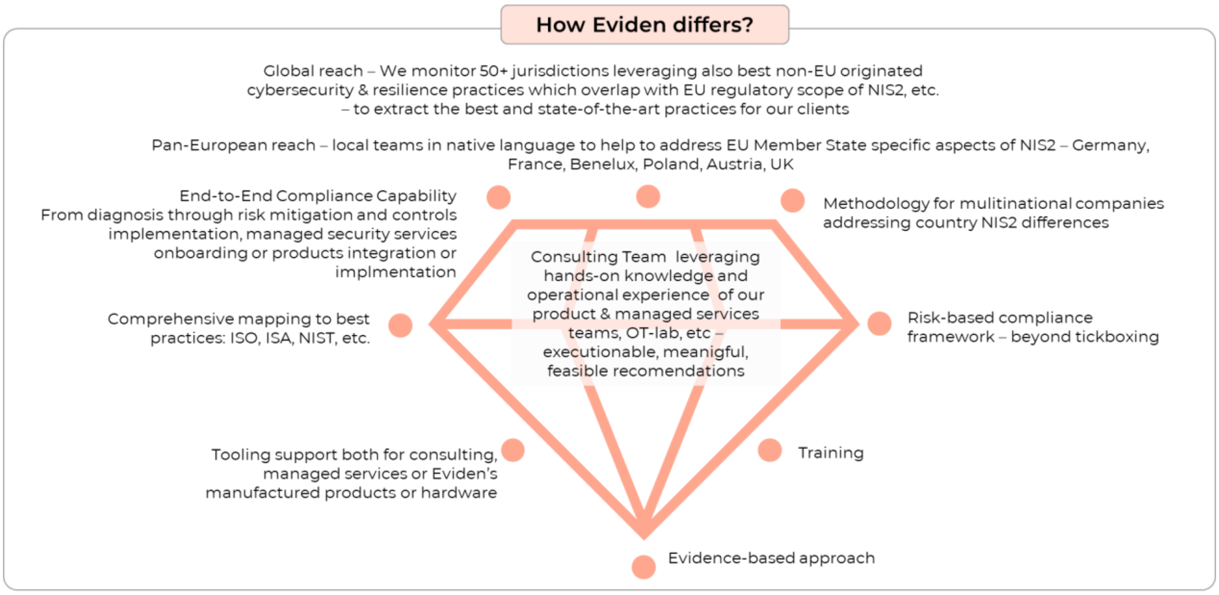
Our advisory engagements work as an entry point of proper tailoring customer needs before any product or service whether ours or our competitors is proposed to the customers, to make sure that before following larger engagements, including integration and MSS (Managed Security Services) business is really justify by business case, organisations strategy or need which is not properly addressed or discovered. We provide broader context, sometimes readdressing initial customer needs after briefing what is challenge or problem to solve – to discover the real one which sometime not visible to our customers at the beginning.

By providing deep insights into security challenges, we guide customers towards successful implementation of new security initiatives. Our custom-built solutions directly address specific client security concerns, fostering trust and solidifying our position as a reliable partner.

Our initial engagements begin with a thorough understanding of the organisation's unique needs. This ensures our solutions are perfectly tailored to your specific challenges before any product or service is recommended. Following the initial engagement, we offer a seamless transition to larger, ongoing services such as security integration and managed security services (MSS).

Overview of our unique capabilities and differentiators of Eviden's value proposition are summarized below on

Figure 20 Elements of Eviden's NIS2 compliance offerings' unique value proposition



How Eviden differs?

Global reach – We monitor 50+ jurisdictions leveraging also best non-EU originated cybersecurity & resilience practices which overlap with EU regulatory scope of NIS2, etc. – to extract the best and state-of-the-art practices for our clients

Pan-European reach – local teams in native language to help to address EU Member State specific aspects of NIS2 – Germany, France, Benelux, Poland, Austria, UK

End-to-End Compliance Capability From diagnosis through risk mitigation and controls implementation, managed security services onboarding or products integration or implmentation

Methodology for mulitinational companies addressing country NIS2 differences

Consulting Team leveraging hands-on knowledge and operational experience of our product & managed services teams, OT-lab, etc – executionable, meanigful, feasible recomendations

Comprehensive mapping to best practices: ISO, ISA, NIST, etc.

Risk-based compliance framework – beyond tickboxing

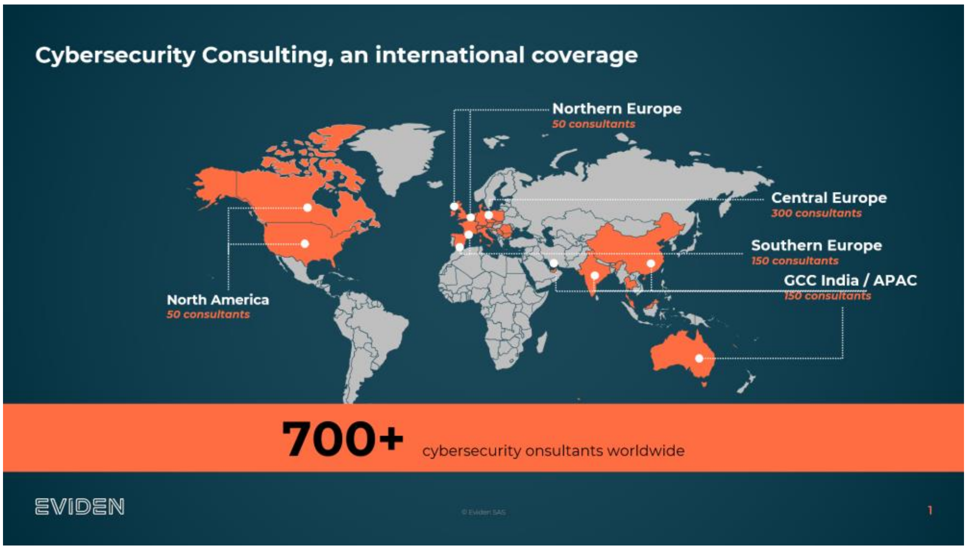
Tooling support both for consulting, managed services or Eviden's manufactured products or hardware

Training

Evidence-based approach

Source: Eviden

Figure 21 Eviden's cybersecurity consulting international coverage

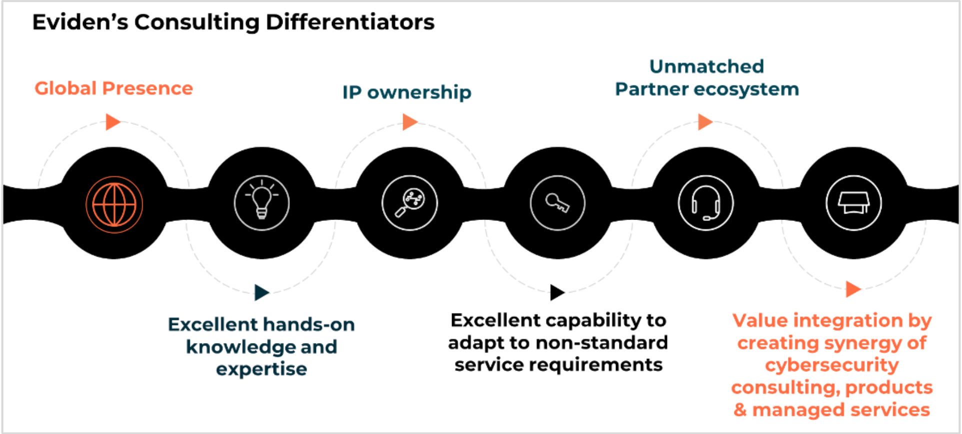


Cybersecurity Consulting, an international coverage

700+ cybersecurity onsultants worldwide

Source: Eviden

Figure 22 Eviden's consulting specific differentiators



Eviden's Consulting Differentiators

Global Presence

IP ownership

Unmatched Partner ecosystem

Excellent hands-on knowledge and expertise

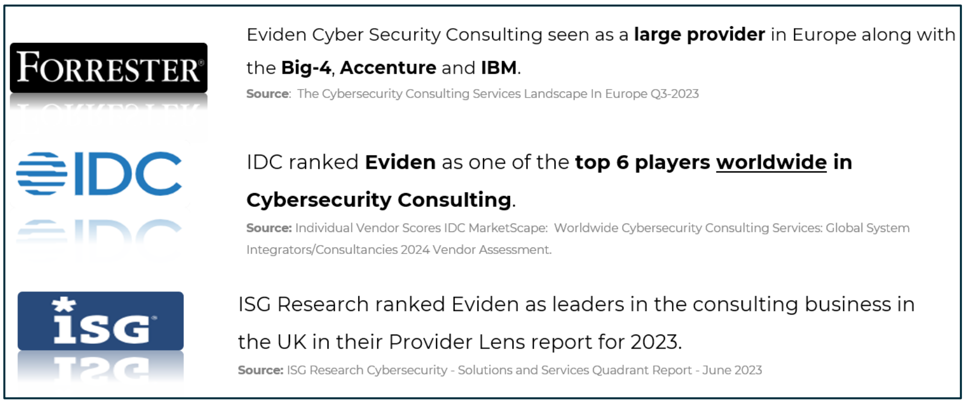
Excellent capability to adapt to non-standard service requirements

Value integration by creating synergy of cybersecurity consulting, products & managed services

Source: Eviden

Our tailored solutions demonstrate commitment to addressing specific client concerns, fostering trust as a reliable partner, which is being notice by market analyst as shown below:

Figure 23 Eviden's cybersecurity consulting rating by market analyst



FORRESTER

Eviden Cyber Security Consulting seen as a **large provider** in Europe along with the **Big-4**, **Accenture** and **IBM**.

Source: The Cybersecurity Consulting Services Landscape In Europe Q3-2023

IDC

IDC ranked **Eviden** as one of the **top 6 players worldwide in Cybersecurity Consulting**.

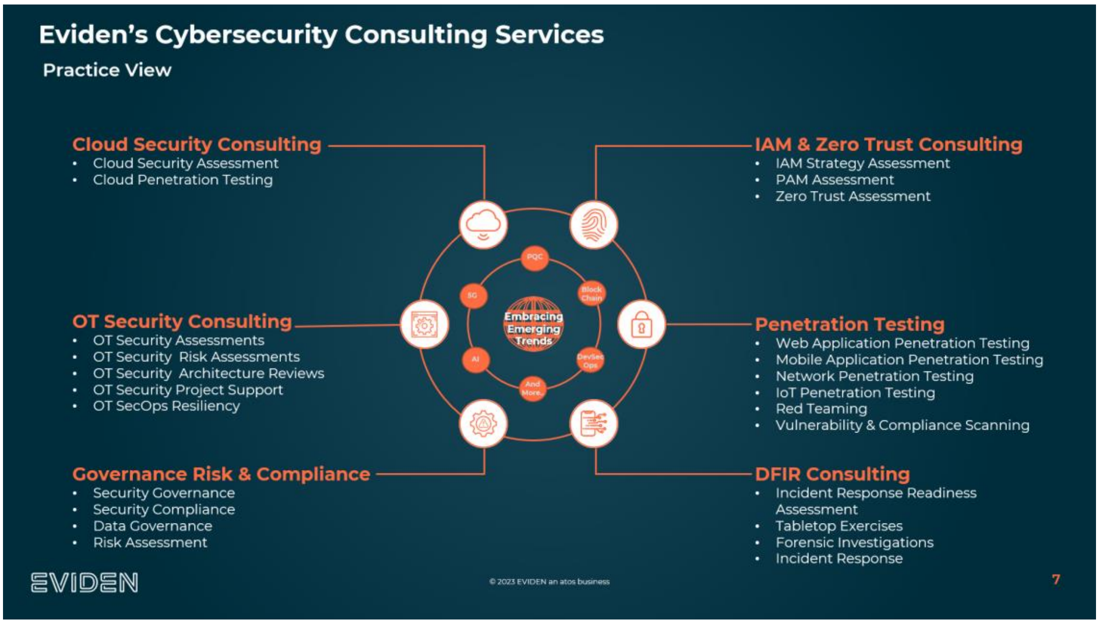
Source: Individual Vendor Scores IDC MarketScape: Worldwide Cybersecurity Consulting Services: Global System Integrators/Consultancies 2024 Vendor Assessment.

ISG Research ranked Eviden as leaders in the consulting business in the UK in their Provider Lens report for 2023.

Source: ISG Research Cybersecurity - Solutions and Services Quadrant Report - June 2023

Source: Eviden

Figure 24 Overview of current Eviden's Consulting Services portfolio.



Eviden's Cybersecurity Consulting Services

Practice View

Cloud Security Consulting
- Cloud Security Assessment
- Cloud Penetration Testing

IAM & Zero Trust Consulting
- IAM Strategy Assessment
- PAM Assessment
- Zero Trust Assessment

OT Security Consulting
- OT Security Assessments
- OT Security Risk Assessments
- OT Security Architecture Reviews
- OT Security Project Support
- OT SecOps Resiliency

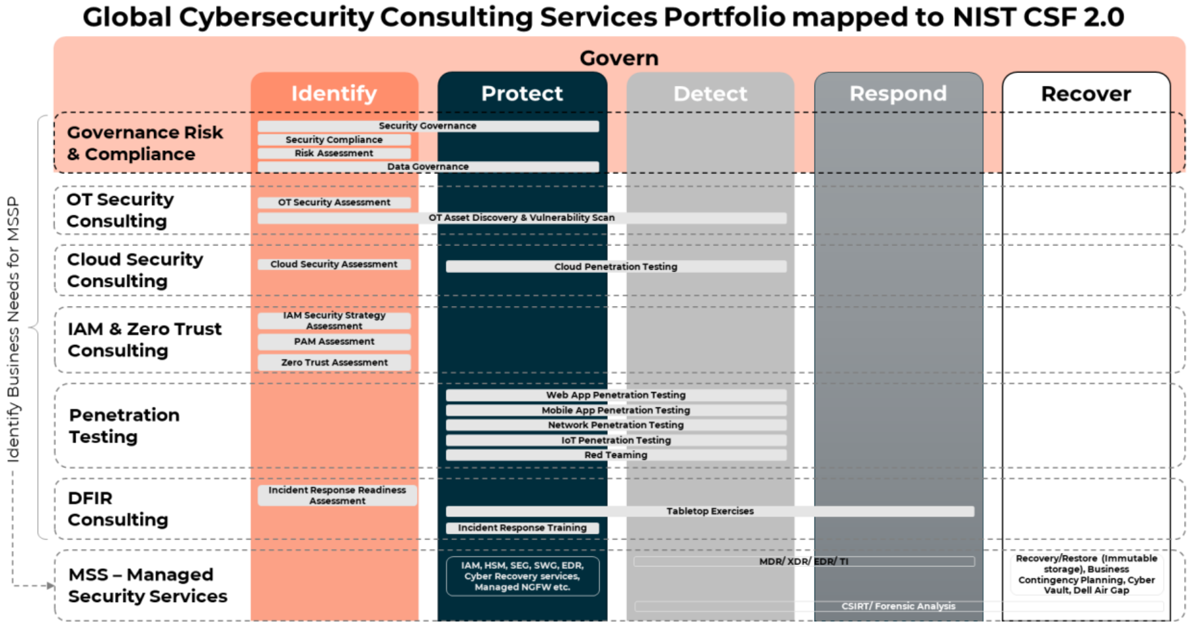
Penetration Testing
- Web Application Penetration Testing
- Mobile Application Penetration Testing
- Network Penetration Testing
- IoT Penetration Testing
- Red Teaming
- Vulnerability & Compliance Scanning

Governance Risk & Compliance
- Security Governance
- Security Compliance
- Data Governance
- Risk Assessment

DFIR Consulting
- Incident Response Readiness Assessment
- Tabletop Exercises
- Forensic Investigations
- Incident Response

Source: Eviden

Figure 25 Eviden's Consulting Services mapped to NIS2 CSF 2.0.



Global Cybersecurity Consulting Services Portfolio mapped to NIST CSF 2.0

	Govern				
	Identify	Protect	Detect	Respond	Recover
Governance Risk & Compliance	Security Governance Security Compliance Risk Assessment Data Governance				
OT Security Consulting	OT Security Assessment OT Asset Discovery & Vulnerability Scan				
Cloud Security Consulting	Cloud Security Assessment	Cloud Penetration Testing			
IAM & Zero Trust Consulting	IAM Security Strategy Assessment PAM Assessment Zero Trust Assessment				
Penetration Testing		Web App Penetration Testing Mobile App Penetration Testing Network Penetration Testing IoT Penetration Testing Red Teaming			
DFIR Consulting	Incident Response Readiness Assessment	Tabletop Exercises Incident Response Training			
MSS – Managed Security Services		IAM, HSM, SEG, SWG, EDR, Cyber Recovery services, Managed NGFW etc.	MDR/ XDR/ EDR/ TI CSIRT/ Forensic Analysis		Recovery/Restore (Immutable storage), Business Contingency Planning, Cyber Vault, Dell Air Gap

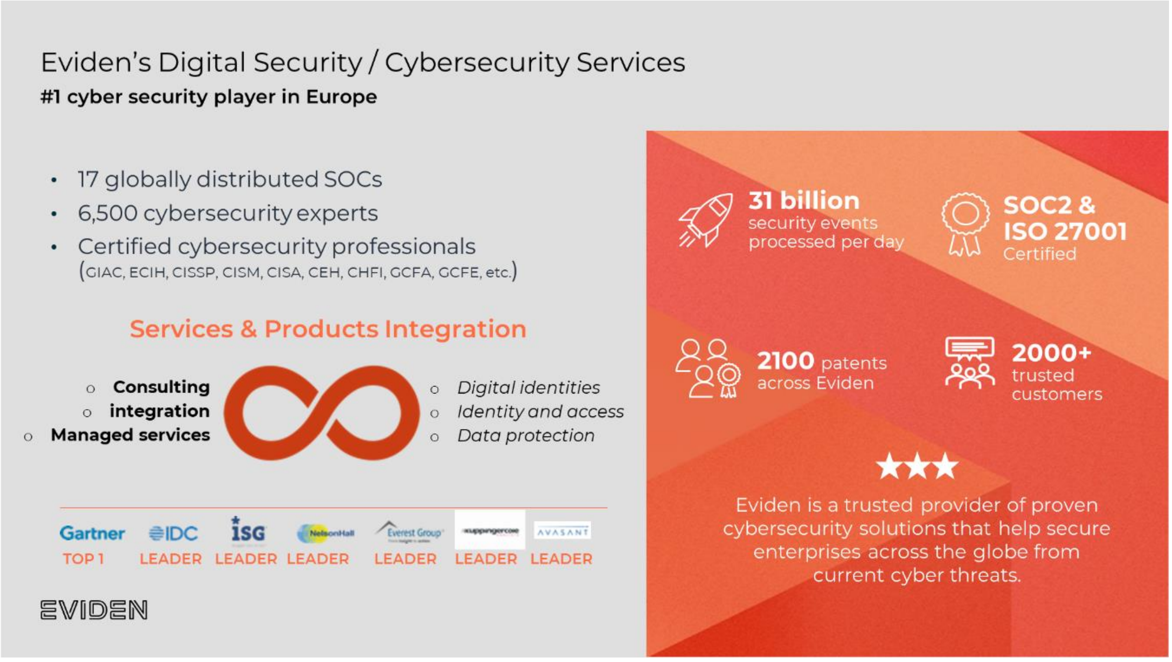
Source: Eviden

9.2 Managed services capability

Our consulting services are standalone part of Eviden cybersecurity services portfolio, but they are also preceding or serve customers as value added to Eviden's managed security services which are onboarded to Eviden customers with ecosystem of Eviden's own manufactured products, hardware or software supporting Eviden services. Analogically Eviden is constantly developing its ecosystem of R&D Centers, Start-ups, and Partners. Overview of Manged Services is presented in the figure below.

Part of Eviden's global network of cloud centres and connected with its 17 SOC (security operation centres) managed by over 6,500 security specialists.

Figure 26 Eviden's managed security services capabilities



Eviden's Digital Security / Cybersecurity Services

#1 cyber security player in Europe

- 17 globally distributed SOCs
- 6,500 cybersecurity experts
- Certified cybersecurity professionals (GIAC, ECIH, CISSP, CISM, CISA, CEH, CHFI, GCFA, GCFE, etc.)

Services & Products Integration

- **Consulting**
- **integration**
- **Managed services**

- *Digital identities*
- *Identity and access*
- *Data protection*

31 billion security events processed per day

SOC2 & ISO 27001 Certified

2100 patents across Eviden

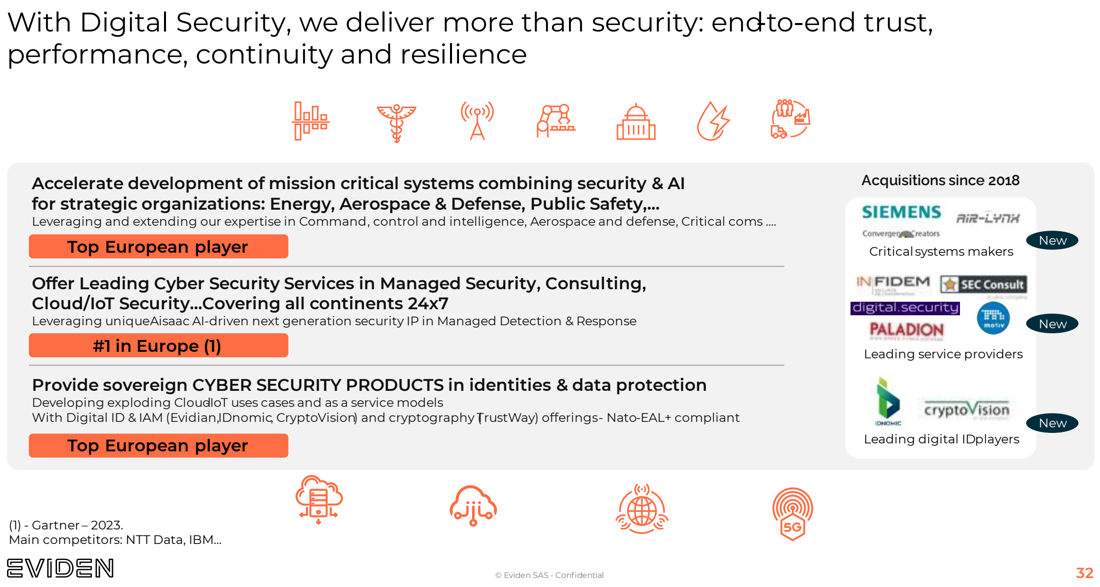
2000+ trusted customers

★★★

Eviden is a trusted provider of proven cybersecurity solutions that help secure enterprises across the globe from current cyber threats.

Source: Eviden

Figure 27 Eviden's rating and synergies



With Digital Security, we deliver more than security: endto-end trust, performance, continuity and resilience

Accelerate development of mission critical systems combining security & AI for strategic organizations: Energy, Aerospace & Defense, Public Safety,...
Leveraging and extending our expertise in Command, control and intelligence, Aerospace and defense, Critical coms ....

Top European player

Offer Leading Cyber Security Services in Managed Security, Consulting, Cloud/IoT Security...Covering all continents 24x7
Leveraging uniqueAisaac AI-driven next generation security IP in Managed Detection & Response

#1 in Europe (1)

Provide sovereign CYBER SECURITY PRODUCTS in identities & data protection
Developing exploding CloudIoT uses cases and as a service models
With Digital ID & IAM (Evidian,IDnomic, CryptoVision) and cryptography (TrustWay) offerings- Nato-EAL+ compliant

Top European player

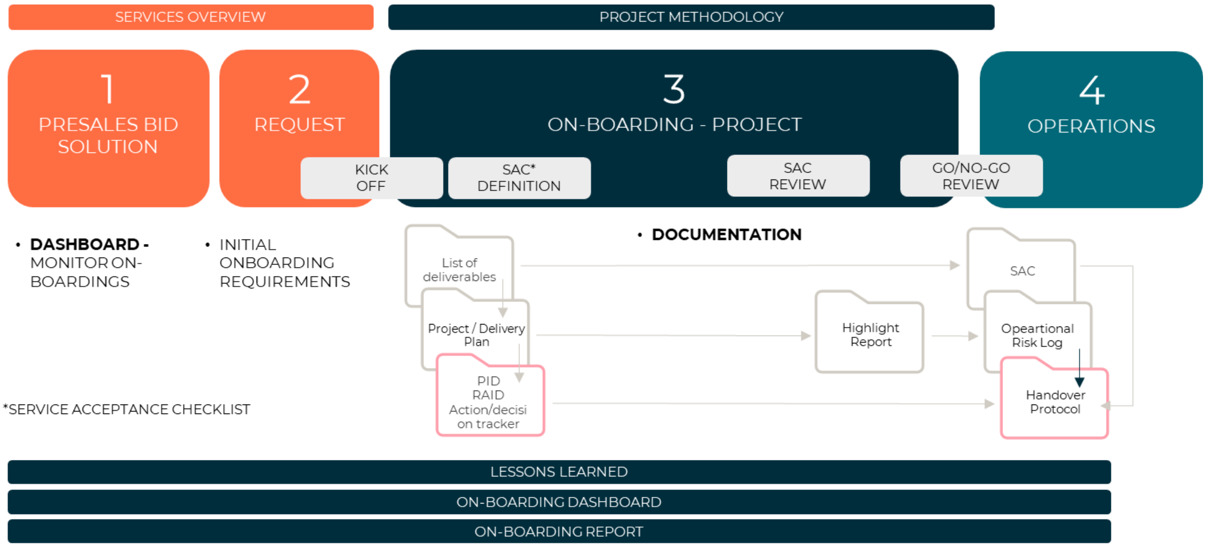
Acquisitions since 2018

(1) - Gartner – 2023.
Main competitors: NTT Data, IBM...

Source: Eviden

Typical onboarding on Eviden's managed security services lasts usually from 2 to 12 months depending on complexity and scope of services to implemented via two main processes: transformation or transition.

Figure 28 Typical process of onboarding Eviden's Managed Security Services for NIS2



Source: Eviden

10 NIS2 in questions & answers

Below for quick reference we summarise key questions and answers on NIS2 compliance contained in this whitepaper.

Table 11 Key questions and answers related to NIS2 Directive

Questions	Aspect / Chapter	EU NIS 2 Directive summarized short answer
Where to find official text of the and identification of NIS2 Directive?	Identifier	Directive (EU) 2022/2555 is the official identification in European Journal of Laws
What is exact title of the Directive?	Title	On measures for a high common level of cybersecurity across the Union (NIS 2 Directive)
I do not understand some of terms and definitions which are used, where can I find them?	Glossary, Legal definitions of NIS2	All necessary terms are clarified in Glossary Section NIS2 legal definitions are contained in the Article 2 of the Directive
What is the date of adoption of the Directive	Date of adoption	14 December 2022
Since when Directive is in force?	Date in force	16 January 2023
What are the deadlines for EU 27 Member States competent authorities to transpose (translate and publish official requirements on the country level)	Transposition date	17 October 2024, 27 EU Member States shall adopt and publish the measures necessary to comply with this Directive. apply those measures from 18 October 2024 Directive (EU) 2016/1148 (NIS1 or NISD) is repealed with effect from 18 October 2024

Questions	Aspect / Chapter	EU NIS 2 Directive summarized short answer
What the deadline before which I should be compliant?	Country level deadline in transposed legislation.	The date, which is the milestone for being compliance ready may slightly differ per given EU Member State.
	Objective	Setting out minimum rules regarding the functioning of a coordinated regulatory framework, by: • laying down mechanisms for effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations • providing effective remedies and enforcement measures which are key to the effective enforcement of those obligations. • to eliminate fragmentation of the internal market and can have a prejudicial effect on its functioning, affecting the cross-border provision of services and the level of cyber resilience. • aims to overcome the shortcomings of the differentiation between operators of essential services and digital service providers
What organisations, companies or institutions are in the scope of NIS2 Directive?	Sectors in Scope	Expands the scope in comparison to former NIS Directive from Operators of Essential Services and Digital Service Providers to so-called Essential and Important entities in sectors of high criticality listed in Annex I and other critical sectors listed in Annex II
What if my business operates in more than one country?	Main jurisdiction and territory in case of more than one country	According to the requirements of the specific article of NIS2 there are principles specifying applicable main jurisdiction and proceeding in the case of multinational companies. Please contact us for your specific use case using the contact below. We have standardised approach for such organisations based on our experience from our projects.
My business is outside EU do I need to comply?	Jurisdiction territorial scope	Yes, for further details refer to NIS2 Article 26 and Section 2.6.2 of this document.
Why I need to comply with NIS2 Directive? Are cyberattacks a real threat for my organisation? Are the cyber threats landscape, trends, attacks evolving so quickly in my industry, sector, or subsector? Are there any data or reports supporting the real cyber risk level for my industry to support decision making?	Industry specific cyber risk landscape reports, aggregated data.	Please refer to Industry Cyber Landscape in Section 6.1 of this document. There are numerous reports published each year on cyber threat security landscape. Please refer to Section 12 for specific references and further reading.
What the typical concerns or challenges of organisations in scope of NIS2 Directive? What customers tells you?	Voice of the customers, market, or industry chambers, associations or other NIS2 stakeholders	Eviden's customer or industry voice expresses the following challenges (not exhaustive): • They are not aware if they are in scope of NIS2 regulations. • They do not know when the right moment is to do preparation work to assure compliance. • They are afraid of reporting cyber incidents to external competent authority if published, they might impact business, credibility, and reputation.

Questions	Aspect / Chapter	EU NIS 2 Directive summarized short answer
		• Compliance and reporting burden (multiple reporting to various country or countries competent authorities of the same incident, report, etc. • They do not know how to impose on their suppliers - the compliance obligations resulting from NIS2 and how to effectively monitor them. • They do not know what the "reasonable" level should be if compliance cost or investments to be made to assure minimum but sufficient compliance needs. • They do not know how to connect cyber risk analysis, business continuity, supply chain managed into consistent framework to justify risk-based spending on compliance ("this is justified amount for which I am able to comply"). • They are afraid how to collect evidence, how to perform documented, reasonable, balanced risk assessment to prove that implemented countermeasures are adequately, proportionally addressing the cybersecurity & cyber resilience risks
Are there penalties of sanctions for non-compliance with NIS2?	Sanctions or Penalties for the organisation (entity)	Administrative fines: • of a max of at least 10 mln EUR or of a max of at least 2% for Essential Entities, • of a max of at least 7 mln EUR or of a max of at least 1.4 % for Important Entities) of the total worldwide annual turnover in the preceding financial year of the undertaking, to which the respective entity belongs, whichever is higher.
Is there personal liability as element of penalties of the management bodies (board members, executives or another indicated person?)	Personal accountability for non-compliance	Yes, there is also personal liability for non-compliance apart from legal entity accountability.
How compliance will be enforced by Regulator? Will there be any regulatory audits?	Ex ante and Ex post regulatory supervision	Yes, there are two main types of regulatory activities: • For essential entities: ex ante & ex post (anytime possible, before, during or after the incident) or • For important entities: ex post only (regulatory audit, supervision activities after incident happened)
Will there be any obligation for regulatory reporting and collecting evidence?	Incident Reporting, Compliance Reporting	Yes, please refer to Article 23 and Section 4.4 of this document.
What needs to be done to comply with NIS2?	Requirements in the Directive (before the transposition is made).	Follow articles 20-24 of NIS2 Directive by implementing are stating what needs to be done to comply with NIS2 • Governance structure including management bodies oversight over status of compliance and implementation of the requirements. • Adopt 10 risk management measures cybersecurity framework, risk management, incident response, BCM/DR Cyber Recovery process, Third Party Supply Chain Cyber risk, vulnerability mgt, secure development process (DevSecOps), MFA, Access Control, Encryption, HR security, Dependent of the given Member State approach.

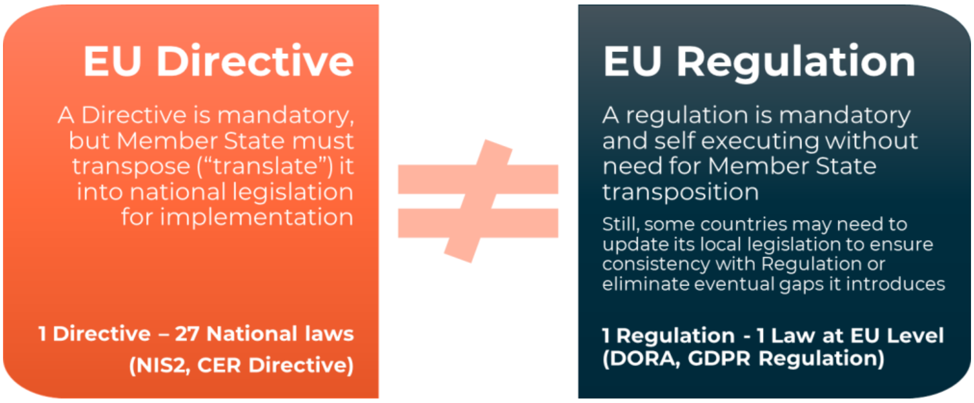
Questions	Aspect / Chapter	EU NIS 2 Directive summarized short answer
Where can I find the status of transposition in my countries	Transposed requirements of NIS2 in the given country law	Our Eviden's Global Governance Risk Compliance Practice being part Cybersecurity Services Business Line is monitoring progress of NIS2 Transposition in most of the member states, please use below contact details for most up to date information.
Is there any guidance of EU or Member State level specifying in more details on how to implement all the requirements of NIS2 Directive to compliant with the principle of proportionality?	NIS2 Delegating Act	As of publication date of this Whitepaper, still NIS2 delegation act is not yet published. Please subscribe to our newsletter below to be informed when it is published.
What should I do now? What are the next steps?	Next decision & actions	Consider training and awareness or assistance of credible and trusted partner on your NIS2 Compliance journey.
How Eviden can help to our organisation regarding NIS2 Compliance?	Eviden approach to NIS2 Directive Eviden NIS2 Cybersecurity Services, Products	Eviden's approach to compliance assurance is described in Section 6 of this document
Is Eviden assisting any other upcoming European Regulations like DORA, CER Directive, Cyber Resilience Act, AI Act, etc?	Eviden EU-Regulations Cybersecurity Services & Products	Eviden's approach to other EU regulatory compliance assurance is described in Section 9.1 of this document
How can I contact your advisor to get more details on NIS2 journey to compliance and related challenges?	Contact Eviden Trusted Advisor	Please contact respective Eviden representative under yourNIS2trustedadvisor@eviden.com for any further details, questions you might have. If you want to be informed as soon as delegating act will be published or order to receive additional information related to NIS2 implementation progress in your country and for any other news in the domain of other upcoming EU Regulations compliance, please sign-up for subscription here: eureg@eviden.com

11 Glossary facilitating reading this document

With each new Directive or Regulation or in general when compliance with regulations is concerned, there is specific legal language used which precisely defines used terms. To assist the reader in understanding of NIS2 Directive requirements and this whitepaper the following definitions, acronyms are used.

First key definition is to understand what Directive is and what is Regulation in EU Law Making process and what are differences between them, what is explained on **Error! Reference source not found.**.

Figure 29 Differences between Directive & Regulation in EU Law making process.



EU Directive

A Directive is mandatory, but Member State must transpose ("translate") it into national legislation for implementation

1 Directive – 27 National laws (NIS2, CER Directive)

≠

EU Regulation

A regulation is mandatory and self executing without need for Member State transposition

Still, some countries may need to update its local legislation to ensure consistency with Regulation or eliminate eventual gaps it introduces

1 Regulation - 1 Law at EU Level (DORA, GDPR Regulation)

Source: Eviden's own elaboration

Table 12 Key definitions facilitating understanding of Eviden's NIS2 Whitepaper

Definition	Meaning
Directive	A "directive" is a legislative act that sets out a goal that EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals[6]. More information is contained in official EU Glossary.[7]
Regulation	A "regulation" is a binding legislative act. It must be applied in its entirety across the EU Member States[8].
Recommendation	Recommendations are one of two forms of non-binding EU acts, the other form being Opinions. Although Recommendations do not have legal consequences, they may offer guidance on the interpretation or content of EU law. A recommendation allows the institutions to make their views known and to suggest a line of action without imposing any legal obligation on those to whom it is addressed.
Delegated Act	Delegated acts are non-legislative acts adopted by the European Commission that serve to amend or supplement the non-essential elements of the legislation[9].
Transposition	Transposition is the process of incorporating EU directives into the national laws of EU Member States.[10]
Recital (Motive)	The 'recitals' (called also 'motives') are the part of the in Directive or Regulation placed before its articles which contain the statement of reasons for its adoption.
Repeal	Withdrawal of Directive or Regulation or substitution by new one (like in case of NIS1 which will be replaced by NIS2 Directive since 18th of October 2024.
Competent Authorities	Authorities appointed by Member States (governmental level) to supervise the essential and important entities' compliance with transposed NIS2 Directive into their country-level laws

[6] Source: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en
[7] Source: https://eur-lex.europa.eu/EN/legal-content/glossary/directive.html
[8] Source: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en
[9] Source: https://eur-lex.europa.eu/EN/legal-content/glossary/delegated-acts.html
[10] Source: https://eur-lex.europa.eu/EN/legal-content/glossary/transposition.html

Definition	Meaning
Proportionality principle	Proportionality is a general principle of EU law. It restricts authorities in the exercise of their powers by requiring them to strike a balance between the means used and the intended aim. Safeguards accompanying a measure can support the justification of a measure. Proportionality principle in NIS2 is addressed in Recitals (21), (81), (133), (142) and in Art. 21.1 on Cybersecurity risk management measures, especially in connection with Recital (81): (81) In order to avoid imposing a disproportionate financial and administrative burden on essential and important entities, the cybersecurity risk-management measures should be proportionate to the risks posed to the network and information system concerned, taking into account the state-of-the-art of such measures, and, where applicable, relevant European and international standards, as well as the cost for their implementation.
European Standard	standard' means a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory, and which is one of the following: a) standard adopted by a European standardisation organization[11]: CEN - European Committee for Standardisation, CENELEC - European Committee for Electrotechnical Standardisation, ETSI - European Telecommunications Standards Institute
International Standard	(a) 'international standard' means a standard adopted by an international standardisation body[12], i.e.: ISO - the International Organisation for Standardisation, IEC - the International Electrotechnical Commission, ITU -the International Telecommunication Union
ENISA	The European Union Agency for Cybersecurity (official website: https://www.enisa.europa.eu/) is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services, and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow[13].

For further information please contact Eviden's experts.

12 References and further reading

12.1 Cyber-attack tables – sources

Sources for Table 7 Overview of research on real cybersecurity threats in critical sectors of Essential Entities and Table 8 Overview of research on real cybersecurity threats in sectors of Important Entities:

https://www.enisa.europa.eu/publications/
https://www.cisa.gov/
https://www.proofpoint.com/us/blog/threat-insight
https://cloud.google.com/blog/topics/threat-intelligence
https://www.conquer-your-risk.com/
https://www.darkreading.com/cyberattacks-data-breaches
https://blog.talosintelligence.com/
https://www.splunk.com/en_us/resources.html?search=threats
https://attack.mitre.org/
https://www.cobalt.io/resources
https://www.sans.org/
https://www.mandiant.com/resources

[11] Source: in Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, in Article 2, point (1).
[12] Source: Regulation (EU) No 1025/2012, as above.
[13] Source: https://www.enisa.europa.eu/about-enisa/regulatory-framework

12.2 Industry specific impacts of cyber attacks

Sources for threats impact description of cyber-attacks per industry for Table 7 Overview of research on real cybersecurity threats in critical sectors of Essential Entities and Table 8 Overview of research on real cybersecurity threats in sectors of Important Entities:

Energy:
https://www.politico.eu/article/energy-power-europe-grid-is-under-a-cyberattack-deluge-industry-warns/

Health:
Ransomware attack impact on Health industry:
https://www.bbc.com/news/uk-england-kent-68284475
https://www.bbc.com/news/articles/cd11v377eywo

Water
https://waterfm.com/what-is-the-state-of-cyber-risk-in-the-water-sector/
https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/
https://www.cbsnews.com/news/cyberattacks-on-water-systems-epa-utilities-take-action/
https://www.govtech.com/security/federal-agency-warns-water-utilities-against-cyber-attacks
https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/
https://www.theregister.com/2024/04/17/russia_sandworm_cyberattacks_water/
https://watereurope.eu/how-can-we-fight-cyberattacks-to-water-infrastructures/

Stop-IT initiative - focuses on the strategic, tactical, and operational protection of critical water infrastructures against physical and cyber threats, more details here:
https://stop-it-project.eu/
https://erncip-project.jrc.ec.europa.eu/system/files/1_Cyber%20security%20in%20water%20sector_STOP-IT%20project_Rita%20Ugarelli.pdf

Manufacturing
https://www.theregister.com/2024/02/27/manufacturing_sector_malware/

Transport
https://cyberconflicts.cyberpeaceinstitute.org/impact/sectors/transportation
https://www.ptsecurity.com/ww-en/analytics/cyber-threats-in-the-transport-sector-2023/

Space
https://www.politico.com/news/2024/03/25/satellite-cyber-threat-00148672
https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites

Postal & Courier Services
Lessons from the Royal Mail Ransomware Attack - TechHQ
https://www.theguardian.com/business/2023/jan/12/royal-mail-ransomware-attackers-threaten-to-publish-stolen-data
https://www.strategic-risk-global.com/catastrophe-risk/royal-mail-cyber-incident-causes-wide-spread-disruption/1443507.article
https://therecord.media/ukraine-cyberattacks-energy-postal-transportation

Food
https://cybersecurityguide.org/industries/food-and-agriculture/

https://www.food-safety.com/articles/8800-cyber-threats-impacting-the-food-and-agriculture-sector
https://gca.isa.org/blog/cybersecurity-in-food-processing-a-hidden-battle-for-safe-sustenance
https://arxiv.org/html/2403.08036v1
https://www.intertek.com/blog/2023/2023-11-07-cybersecurity-food/
https://www.just-food.com/features/tech-leaves-food-industry-more-exposed-to-cybersecurity-threat/
https://link.springer.com/article/10.1007/s44187-023-00071-7

Research
https://applied-risk.com/resources/cyber-security-research-and-development
https://workingcapitalreview.com/2018/10/the-effect-of-cybersecurity-concerns-on-research-and-development/

Chemical industry
https://www.chemengonline.com/cyber-threats-facing-the-chemicals-industry/

12.3 Additional EU level information

National coordination centers:
https://cybersecurity-centre.europa.eu/nccs-0_en

13 List of Figures, Tables and Diagrams

13.1 List of Figures

13.2 List of Tables

13.3 List of Diagrams

Follow Eviden Digital Security:
eviden.com