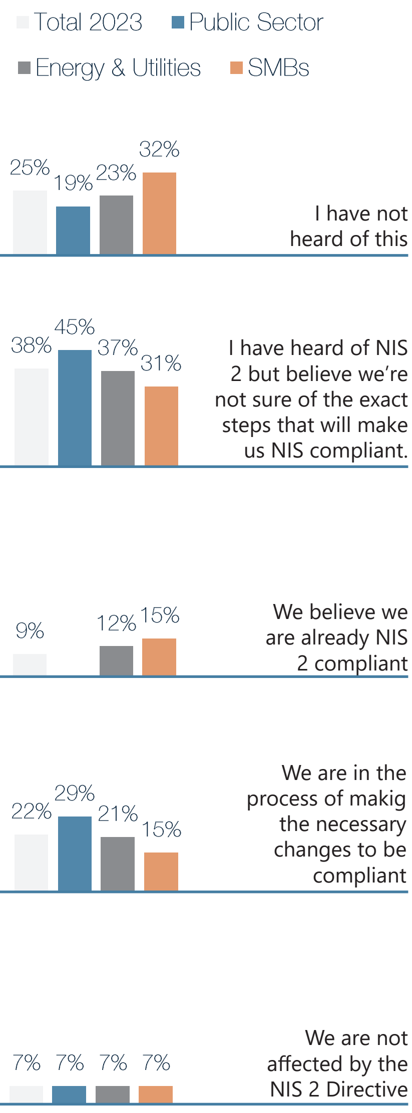
Getting Ready for the NIS2 Directive

clavister®

Summary

Which of the following best describes your position on the NIS2 Directive



Source: Clavister Cyber Security Market Survey 2023

In January 2023, the European Union's member states implemented an update to the 2016 Network and Information Systems (NIS) Directive. This legislation aims to establish a uniformly high level of cyber security throughout the member states and remove some of the ambiguities associated with the original version. The updated NIS2 Directive enhances security protocols, simplifies the obligations for incident reporting, and imposes more rigorous oversight measures. These changes are designed to protect critical infrastructure from threats such as supply chain weaknesses, ransomware, and various other cybersecurity risks.

All 27 EU member states must incorporate the NIS2 Directive into their national laws by October 2024. However, the market is not yet ready for it. In Clavister's 2023 Cyber Security Market Survey, 25% of cyber security professionals admitted that they haven't even heard about NIS2.

In this paper, we provide you an overview of the NIS2 Directive, helping you to assess whether you fall under the directive or not and list some essential steps or best practices to help you on your NIS2 journey.

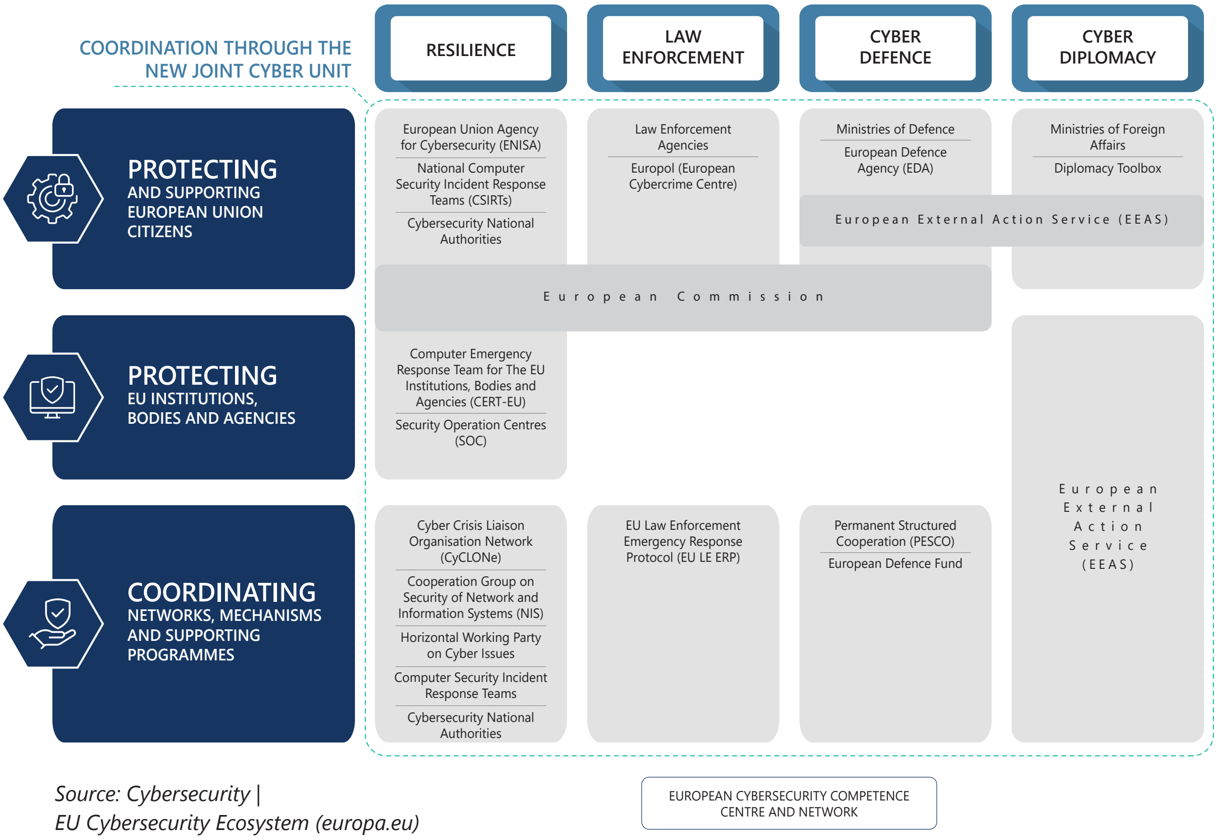
clavister

How European Union aims to bolster cyber security

The new EU Cyber Security Strategy

Recognising the ever-growing threat which cyber-crime poses for the economic and societal stability of the Union, the EU is leading the charge to promote cyber resilience across member states. The new EU Cyber Security Strategy focuses on building collective capabilities to respond to major cyberattacks and working with partners around the world to ensure international security and stability in cyber space. NIS2 is the centre piece of this strategy along with various new regulations that will transform the regulatory landscape and require a culture shift across the whole networking and information security industry.

EU CYBERSECURITY ECOSYSTEM



COORDINATION THROUGH THE NEW JOINT CYBER UNIT

	RESILIENCE	LAW ENFORCEMENT	CYBER DEFENCE	CYBER DIPLOMACY
PROTECTING AND SUPPORTING EUROPEAN UNION CITIZENS	European Union Agency for Cybersecurity (ENISA) National Computer Security Incident Response Teams (CSIRTs) Cybersecurity National Authorities	Law Enforcement Agencies Europol (European Cybercrime Centre)	Ministries of Defence European Defence Agency (EDA) European External Action Service (EEAS)	Ministries of Foreign Affairs Diplomacy Toolbox European External Action Service (EEAS)
	European Commission	European Commission	European Commission	
PROTECTING EU INSTITUTIONS, BODIES AND AGENCIES	Computer Emergency Response Team for The EU Institutions, Bodies and Agencies (CERT-EU) Security Operation Centres (SOC)			European External Action Service (EEAS)
COORDINATING NETWORKS, MECHANISMS AND SUPPORTING PROGRAMMES	Cyber Crisis Liaison Organisation Network (CyCLONe) Cooperation Group on Security of Network and Information Systems (NIS) Horizontal Working Party on Cyber Issues Computer Security Incident Response Teams Cybersecurity National Authorities	EU Law Enforcement Emergency Response Protocol (EU LE ERP)	Permanent Structured Cooperation (PESCO) European Defence Fund	

EUROPEAN CYBERSECURITY COMPETENCE CENTRE AND NETWORK

Source: Cybersecurity | EU Cybersecurity Ecosystem (europa.eu)

The NIS2 Directive – Overview

July 2016

NIS 1 Directive, first EU wide cyber security law

NIS2 regulation was approved by the Council of Ministers and published in the EU Official Journal on 27 December 2022 and thereafter entered into force on 16 January 2023. Member states now have less than a year until it is transposed into national laws, becoming enforceable after that.

> **The emphasis is on harmonisation, standardisation, and cooperation to create a unified and strong cybersecurity posture across Europe.**

Dec 2020

New EU cyber security strategy

Jan 2023

NIS 2 Directive

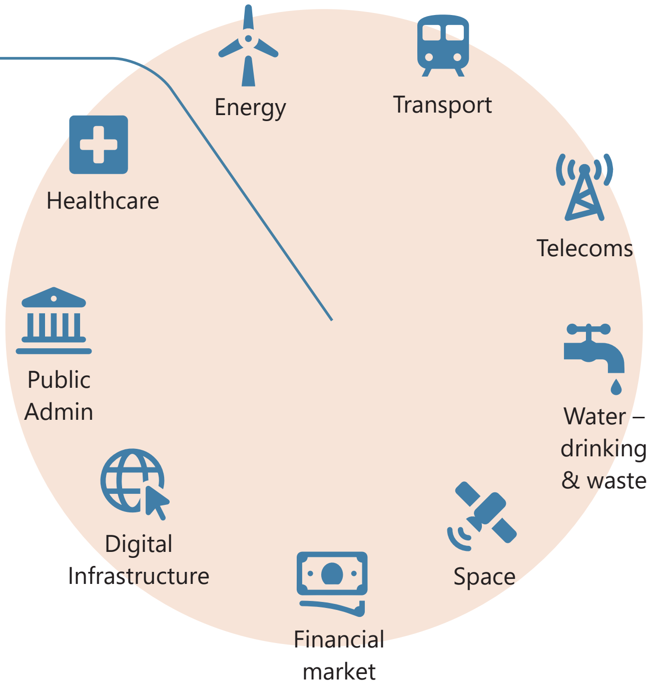
July 2024

NIS 2 Directive transposed in member countries

The NIS2 Directive expands significantly on the sectors impacted as compared to the original NIS Directive. Initially, the NIS Directive identified specific sectors like Healthcare, Transport, Banking and Financial Market Infrastructures, Digital Infrastructure, Water Supply, Energy, and Digital Service Providers as vital, allowing Member States to determine which organisations were critical. The NIS2 Directive is less voluntary and expands significantly wider than its predecessor to include a greater number of sectors, for example social media, managed service providers, waste management, and postal service. It categorises sectors as 'Essential' and 'Important'. The NIS2 Directive mandates that all medium-sized and large enterprises across these categories comply with its regulations. Subcontractors to critical infrastructure including service providers and digital services companies are also covered under NIS 2.

Essential

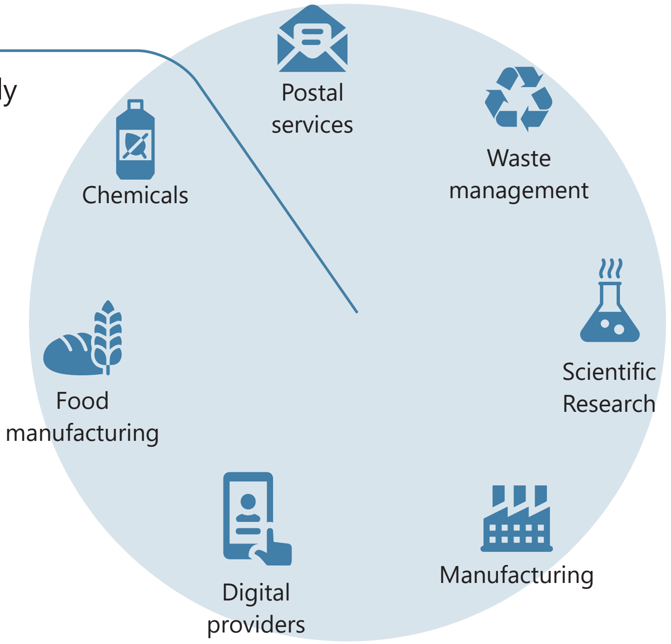
- Size threshold: varies by sector, but generally 250 employees, annual turnover of € 50 million or balance sheet of € 43 million
- Essential entities play a crucial role in maintaining vital functions that are fundamental to the state's stability and well-being. A disruption in their services is expected to have serious consequences for a country's economy or society as a whole.
- Fine – up to € 10 million or 2% of total worldwide annual revenue
  Management can be held liable for infringement



Important

- Size threshold: varies by sector, but generally 50 employees, annual turnover of € 10 million or balance sheet of € 10 million
- These entities are vital, the impact of a disruption in their services may not be as far-reaching or critical as those classified as essential
- Fine – up to € 7 million or 1.4% of total worldwide annual revenue

There are estimated 160,000 organisations to be covered under the NIS2 Directive!



Role of Member States

NIS 2 and Member States’ Role

Member States have the power to characterise sectors for both Essential and Important categories. This indicates the importance of individual Member States, not only in their implementation of the Directive, but also in determining which entities will be in-scope, and how they are classified. There are a few exception to this, for example, regardless of their size public administration will always be regarded as ‘Essential’.

Each member state must adapt its national laws to meet the requirements of the NIS2 Directive. This involves creating or amending laws, regulations, and administrative provisions necessary to comply with the Directive’s stipulations. Member states must set up a national framework for cyber security, which includes designating national competent authorities, single points of contact, and Computer Security Incident Response Teams (CSIRTs).

Member states play a crucial role in strengthening the cybersecurity resilience of the European Union, ensuring a coordinated approach

Proactive Scanning of Public Networks

NIS2 includes a specific section on cybersecurity information sharing arrangement, which member states shall facilitate for essential and important entities and their suppliers. For this, national CSIRTs may carry out proactive non-intrusive scanning of publicly available network and information systems of essential and important entities. It was a gray area in NIS Directive but more clearly defined in NIS 2.

NIS2 applies to any entity providing critical services within an EU member country, regardless of where that entity is located. In other words, any company based outside of the EU could be subject to NIS2 even if they do not have a physical presence in the EU.

Impact on different sectors

Public administration/ Municipalities

Public administration is categorised as 'Essential' under NIS2 Directive. This classification underscores the importance of cyber security and resilience within governmental services and public administration entities.

The final determination, however, would depend on how different member states interprets and implements the directive within the national framework. For example, Swedish Civil Contingencies Agency (MSB), which is the single point of contact for NIS2 in Sweden, municipalities may be classified as essential or important entities if they provide services in any of the sectors covered by NIS2, such as public administration, waste management, drinking water supply and distribution, or social security. The implementation of NIS2 in Sweden is still ongoing, and a governmental inquiry was appointed earlier this year to propose how to transpose the regulation into national law. The inquiry should be completed no later than February 2024. Until then, municipalities and other entities in scope of NIS2 should prepare for the upcoming changes and assess their current level of compliance and security posture.

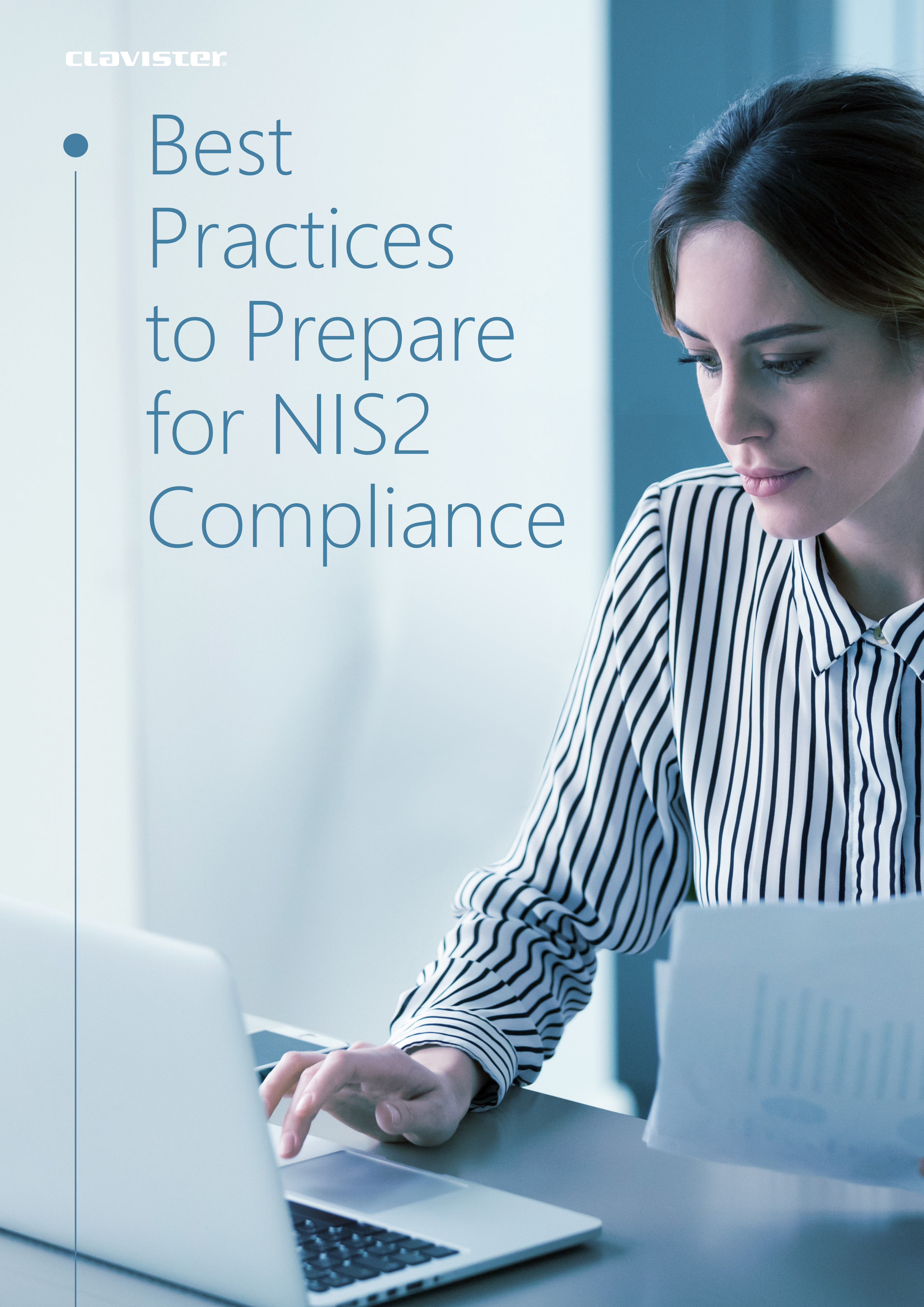
Energy & Utilities

Energy companies were already covered under first NIS Directive, therefore, they already had to deal with their security obligations. With NIS2, energy companies are classified as 'Essential', regardless of company size. Energy sector is part of any nation's critical infrastructure because of which it is also one of the most vulnerable sector for targeted attacks. Russian surveillance of Nordics' energy infrastructure was recently mentioned in a report by Centre for European Reform. NIS2 Directive will impose stricter cyber security risk assessment & management, incident response and incident reporting obligations on energy companies.

NIS2 covers specific utilities for example, water processor and recycling companies that weren't originally covered under NIS or other cyber security legislations. This is because there is a realisation now that these essential services can also be targeted. There has been instances where ransomware attacks have shut down garbage trucks for days from driving. Many utility companies have digitalised their IT and OT infrastructure by deploying Machine-to-machine (M2M) devices and new wireless technologies like 5G, and these new additions increase the cyber risks.

clavister

Best Practices to Prepare for NIS2 Compliance



Risk assessment

- identify, assess and prioritise your risks

It's crucial for your organisation to understand the specific threat landscape that pertains to your sector. For entities providing essential services, the threat actors are often state-sponsored groups who aren't motivated by financial gain but may aim to disrupt operations or cause reputational damage. This may not always involve stealing data; it could be about impacting critical operations. In the manufacturing sector, the theft of intellectual property can be a primary concern. Therefore, it's important to regularly identify and assess cyber risks to stay ahead of potential threats.

Evaluate your security posture

– what's needed to improve it?

Evaluating your security posture is a critical step in enhancing your organisation's cyber defenses. Start by taking stock of what measures you already have in place and pinpointing any vulnerabilities, such as data breaches or unsecured business processes. Conducting a security assessment is invaluable in highlighting areas of concern, like poorly managed passwords or misconfigured and inactive accounts, which are often easy targets for credential theft. By identifying these gaps, you can develop a more informed strategy to strengthen your security infrastructure.

Adopt the zero-trust based approach for cyber security

In today's era of cloud services and remote work, traditional security models designed to protect the borders of an enterprise network fall short. It's advisable to embrace a Zero Trust security model that doesn't automatically trust any entity inside or outside its perimeters. Instead, it employs multiple defensive layers, including enforcing the principle of least privilege, continuous verification, and advanced threat analytics for every access request. Operating under the assumption that a breach is inevitable, Zero Trust strategies concentrate on quickly detecting breaches and minimizing their impact.

Focus on security (software) supply chain

Concerns over supply chain vulnerabilities have significantly influenced the EU's creation of the NIS2 Directive. It's essential to reassess your software supply chain management critically. Integrating a solution for managing sensitive information can play a vital role in reducing these risks. Additionally, ensure that every link in your supply chain, especially subcontractors and smaller vendors, adheres to robust cybersecurity protocols.

Formalise your incident response and reporting plan

The NIS2 Directive mandates more prompt incident reporting procedures so review your event notification, information gathering and reporting processes. 'Essential' entities are required to report an incident and provide early warning to their national CSIRT or authority within 24 hours. Entities are also expected to inform customers about the threat proactively. A comprehensive initial assessment should follow within 72 hours, with a final detailed report due within a month. Additionally, NIS2 has established EU-CyCLONe, operated by ENISA, to facilitate the coordinated response to major cybersecurity incidents and promote information sharing across the EU.

Protect and safeguard high-level access credentials

Attackers often target privileged accounts to execute attacks, compromise vital infrastructure, and interrupt key services. The NIS2 Directive recommends that entities designated as critical restrict the use of high-level administrative accounts and consistently change administrative passwords

What Should be Your Starting point?

Hopefully, you would have started on the NIS 2 Directive compliance journey already, if not the starting point for you is to educate yourself. Understanding the directive and familiarising yourself with the contents of it is the first step. Does our company operate in a sector that is covered by the NIS2 Directive, as we have listed above? If yes, is it categorised as Essential or Important entity? What cyber security measures you already have in place and where are the gaps? Here are some useful links to understand the basics of NIS2:

- The NIS2 Directive – briefing document
- ENISA's NIS Directive tool
- Key focus areas for NIS2 compliance

Liaise with your national agency who would be the single point of contact for NIS2 and would be working on transposing it into national law. Find out the competent authorities for different sectors like ICT, energy, public administration, health and banking. National CSIRT will play an active role in the implementation and supervision of NIS2 so discuss your requirement with them. You can use this link to find out key agencies and status of transposition for your country: State-of-play of the transposition of the NIS Directive

Organisations may need to invest in new technology technologies or services that enhance their ability to detect and respond to incidents. Time is now to be able to have timely implementation. This is where external expertise is needed to assist with compliance.

How can Clavister help?

Speak to your existing cyber security vendor(s) to understand your existing security infrastructure and the gaps to be covered, your starting point should be specific to your requirements.

We, at Clavister are happy to help offer our advise and solutions for:

Layered network security – dual firewalls

Avoid putting all eggs in one basket, to keep the critical infrastructure up and running, use multiple layers of firewalls to spread risk. What will happen if the main organisation-wide firewall cluster goes down, will a water treatment plant, energy production site or the local fire brigade still be up and running? Invest in building redundancy in your infrastructure to reduce and control the impact of a potential cyber attack.

Micro segmentation

Best practice is to segment as far out in the organisation as possible, to avoid relying on central resources. Both physical and logical (VLAN) network segmentation is key. One shall also make sure to not share “common resources” as a municipality wide wireless infrastructure or firewall between the municipality and fully owned private companies, legal NIS2 essential entities.

MFA/ Passwordless

Multi-factor authentication (MFA) is an important aspect of NIS2 as it significantly increases the security of user logins for cloud services and other platforms. NIS2 Directive aims to enhance the security of authentication processes, especially for systems that are critical for the provision of essential services like energy, transport, banking, and healthcare.

ZTNA

Both on application level and network access level. Important in industry OT environment, zero trust identity on legacy ‘non standard’ applications. Also, for entities under NIS2 that rely on external vendors, implementing Zero Trust principles can help manage vendor risk effectively, as it controls access to resources based on continuous verification.

Contact Clavister today for more information
on how we can assist you to get ready for NIS2!

SECURITY BY
SWEDEN

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 • **Fax:** +46 (0)660 122 50 • **Web:** www.clavister.com