WHITEPAPER

Mastering NIS2 Compliance

The ultimate guide
for manufacturers and
machine suppliers

secomea

About Secomea

Founded in 2008, Secomea has been catering to the OT remote access needs of manufacturers and machine builders for over 15 years.

Secomea is a Secure Remote Access (SRA) solution purpose-built for industrial networks and OT equipment. Over 9.500 customers around the world use it every day across thousands of sites to manage remote access to their machines, reduce cybersecurity risks, and prevent downtime.

The content provided in this publication is intended for general informational purposes only and not to be relied upon as legal or other professional advice. Although we endeavor to provide correct and timely information, we cannot guarantee its accuracy as of the date it is received since it may not be up to date with the most recent legal or technical developments. Secomea would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. For additional information, please visit **secomea.com**

The road to overcoming manufacturing challenges to NIS2 compliance

At Secomea, we've been engaging with customers and users since the onset of the NIS2 Directive to support them as they embark on their compliance journey.

From our conversations with our customers, we see a few main challenges faced by organizations in the manufacturing industry when they confront themselves with the NIS2 Directive.

For the sectors and entities new to the scope, NIS2 compliance appears to be a particularly daunting task

Most of the organizations belonging to the sectors of high criticality included in Annex I (Essential Entities) were already familiar with the first NIS Directive of 2016. Besides, a significant portion of them have been directly affected by the GDPR since 2018, in response to which they have already likely improved their cybersecurity profile and expanded their compliance departments and processes.

On the other hand, the majority of the companies included in the other critical sectors listed by Annex II (Important Entities) are brand new to the situation of having to fulfill the requirements of comprehensive cybersecurity legislation.

To make matters worse, they might not have the skills and resources to prepare themselves properly.

Last but not least, key decision-makers might not be used to actively participating in security conversations.

For these reasons, even knowing where to start can be challenging.

Assessing suppliers' risks is especially difficult for organizations with hundreds of different machine vendors

The NIS2 Directive requires you to gather details regarding the security measures of every supplier and service provider you work with. This involves identifying the crucial third-party assets supporting your essential services, evaluating their cybersecurity protocols, and assessing how they handle vulnerabilities - considering the specific weaknesses associated with their products and services.

The more complex your OT setup, the more demanding is such a task.

A typical manufacturing organization might have 10 to 1000 different machine suppliers whose risk profiles need to be investigated and included in its risk assessment.

This represents a quite complicated and laborious assignment, albeit necessary to prepare the company's risk management strategies (and to comply with the Directive).

Not having national legislation and sector guidelines is frustrating, considering that the clock is ticking

Initiating activities to achieve compliance with the NIS2 Directive sounds like quite a lot of homework to impacted organizations.

Many companies would feel more confident in launching their compliance programs on the basis of local legislation implemented in their country to ensure they take the precise steps needed to comply with their national law.

For the same reason, some organizations would prefer to wait for sector-specific cybersecurity guidelines released by industry authorities outlining concrete rules and requirements that distinctly address their unique characteristics.

However, we'd still encourage you to acknowledge how the NIS2 Directive has already laid down the minimum requirements you need to comply with, so it represents a good outset to kick off your initial activities.

By the time you have implemented those minimum requirements, national legislation will likely have been adopted in your country, and sector-specific guidelines will have been published.

At that point, you will simply have to perform a gap analysis to verify whether additional actions are needed from your side to address the specifications provided at a national level and from industry authorities.

To support you in achieving full compliance, we have compiled this whitepaper covering everything you need to know about the new cybersecurity legislation.

Read on to

- **Learn** what the NIS2 Directive is and why it was needed
- **Understand** if you fall into the scope of the Directive and whether your organization is considered an essential or important entity
- **Familiarize** yourself with the requirements you need to comply with
- **Discover** how you can achieve full NIS2 compliance through 10 steps
- **Find out** how you can prepare for an inspection from the authorities and ensure its successful outcome
- **Get support** in fulfilling your NIS2 obligations by using Secomea to improve your cybersecurity

Table of contents

The genesis of the NIS2 Directive

Striving for cybersecurity resilience

1

secomea

From NIS to NIS2: the evolution of the EU-wide legislation on cybersecurity

Why was the NIS2 Directive needed?

The NIS Directive adopted in 2016 was the first-ever cybersecurity law in the European Union.

Despite its significant accomplishments in increasing Member States' cybersecurity levels, the implementation of the NIS Directive was fragmented and inconsistent across Member States and impacted sectors.

Despite its significant accomplishments in increasing Member States' cybersecurity levels, the implementation of the NIS Directive was fragmented and inconsistent across Member States and impacted sectors.

Moreover, the regulatory framework revealed certain limitations in addressing new cyber threats emerging from society's digital transformation and amplified by the pandemic.

What is the NIS2 Directive?

What we normally refer to as NIS2 is a Directive from the European Union that provides **the new EU-wide legislation on cybersecurity.**

It is commonly known as the NIS **2** Directive because it repeals the previous legislation on the matter, another EU Directive from 2016 "concerning measures for a high common level of security on **N**etwork and **I**nformation **S**ystems (**NIS**)".

The more heavily the European economy relies on digital solutions, the more disruptive cyberattacks could be, even if isolated to a single entity or sector. And that's because their effect could be widespread and impact service delivery across the entire internal market.

To make up for the Directive's ineffectiveness and respond to the evolved cyber-risks landscape, the EU Commission proposed a revision – resulting in the NIS2 Directive – intended to:

- Expand the scope of the legislation to more of the ICT-reliant sectors essential to our economy, such as energy, transport, banking, drinking water, healthcare, manufacturing, food production, digital infrastructure, and so on.
- Add future-proof rules aimed at strengthening entities' cyber resilience.
- Improve Member States' preparedness by requiring them to designate national Computer Security Incident Response Teams (CSIRTs), a competent national Network and Information Systems (NIS) authority, and a single point of contact (SPOC).
- Reinforce Member States' collaboration via the Cooperation Group and the CSIRTs Network to facilitate the exchange of information.

When did it enter into force? And what is your deadline to ensure compliance?

The EU NIS2 Directive entered into force on 16 January 2023 and gave Member States time until 17 October 2024 to transpose its measures into national law. By then, you will need to have ensured NIS2 compliance within your organization.

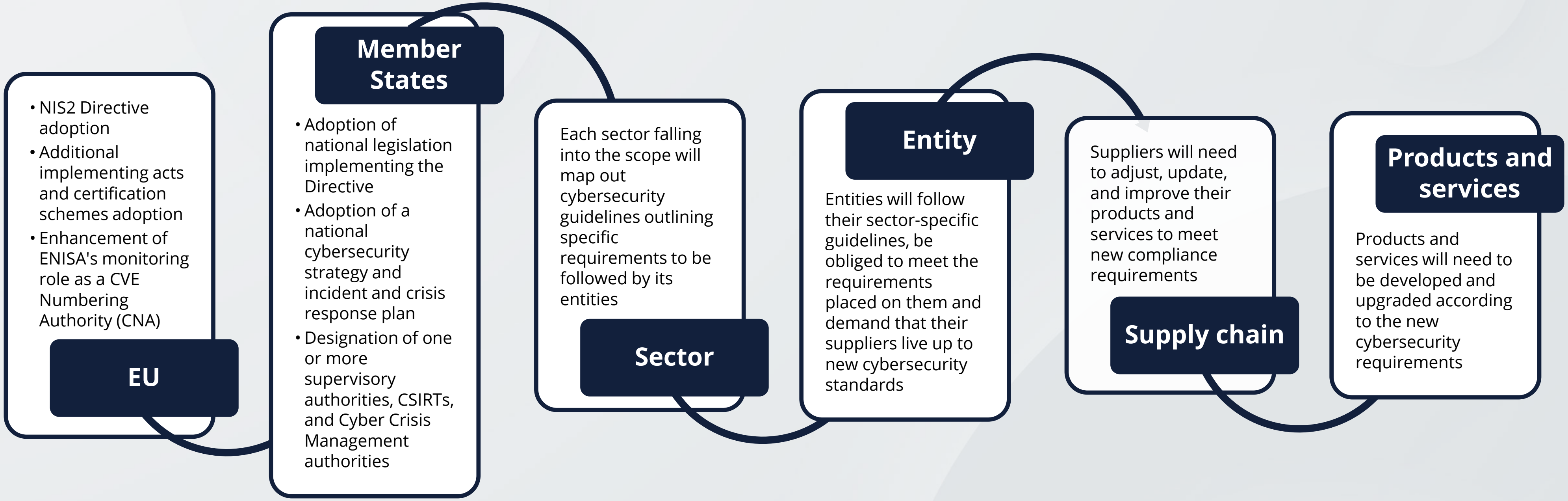
What are the next steps?

- **The role of the EU**

  The Directive laid down general cybersecurity measures, but the EU will also adopt additional implementing acts and certification schemes later on to further specify technical requirements.

  Additionally, the Directive has enhanced the EU Agency for Cybersecurity (**ENISA**)'s role in monitoring Member States' cyber hygiene policies by assigning to the agency new tasks, such as **establishing a European vulnerability database** where entities and their suppliers of network and information systems, as well as the competent authorities and the CSIRTs must report incidents and can disclose and register publicly known vulnerabilities for the purpose to allow users to take appropriate mitigating measures.

  As of January 23rd, 2023, **ENISA is a CVE Numbering Authority (CNA)** for vulnerabilities in information technology (IT) products discovered by EU CSIRTs or reported to EU CSIRTs for coordinated disclosure.



EU

- NIS2 Directive adoption
- Additional implementing acts and certification schemes adoption
- Enhancement of ENISA's monitoring role as a CVE Numbering Authority (CNA)

Member States

- Adoption of national legislation implementing the Directive
- Adoption of a national cybersecurity strategy and incident and crisis response plan
- Designation of one or more supervisory authorities, CSIRTs, and Cyber Crisis Management authorities

Sector

Each sector falling into the scope will map out cybersecurity guidelines outlining specific requirements to be followed by its entities

Entity

Entities will follow their sector-specific guidelines, be obliged to meet the requirements placed on them and demand that their suppliers live up to new cybersecurity standards

Supply chain

Suppliers will need to adjust, update, and improve their products and services to meet new compliance requirements

Products and services

Products and services will need to be developed and upgraded according to the new cybersecurity requirements

As the first (and, until very recently, the only) CNA in Denmark, we at Secomea are thrilled to witness ENISA taking this important step to strengthen the cybersecurity landscape through a more efficient process for reporting vulnerabilities.

- **The role of Member States**

By October 17, 2024, Member States will have to implement the requirements set by the directive internally by adopting national laws.

Besides the national transposition of the Directive, each Member State is also required to

- adopt a national cybersecurity strategy
- designate or establish one or more competent authorities responsible for compliance supervision
- designate or establish a single point of contact that will ensure cross-border cooperation with other Member States and the ENISA
- designate or establish one or more Cyber Crisis Management authorities responsible for the management of large-scale cybersecurity incidents and crises; the representatives of the national Cyber Crisis Management authorities will be part of the EU-CyCLONe (European Cyber Crisis Liaison Organization Network).

- **But that’s not all**

  The competent authority in each sector falling into the scope will be tasked with mapping out the specific cybersecurity requirements to be followed by its entities.

  The entities, in turn, will follow their sector-specific guidelines and demand that their suppliers live up to new cybersecurity standards.

  Finally, suppliers will need to adjust, update, and improve their products and services to meet new compliance requirements.

  As a result, products and services will need to be developed and upgraded according to the new requirements.

2

In or out: assessing your position within the NIS2 Scope

Does your organization qualify as an essential or important entity?

Do you fall within the scope of NIS2?

Which sectors and companies are impacted by the NIS2 Directive?

The sectors falling into the scope of the NIS2 Directive are listed in its Annexes I and II. Annex I covers "sectors of high criticality" and Annex II covers "other critical sectors".

Not all the entities belonging to these sectors fall into the scope of the NIS2 Directive: **only companies that exceed the threshold to be considered a medium-sized enterprise** (i.e., employing more than 50 people or with an annual turnover/balance sheet total exceeding EUR 10 million) are impacted.

However, the Directive lists **some cases** where entities fall into its scope **regardless of their size**. A company that doesn't reach the size threshold is subject to the Directive if:

- is the sole provider of a critical service in a Member State;
- the disruption of the service provided could have a significant impact on public safety, public security, or public health, or it could induce a significant systemic risk;
- is critical because of its specific importance at a national or regional level for the particular sector or type of service;
- is a public administration entity at a national or regional level.

Essential entities and important entities

All entities belonging to the sectors listed in these Annexes and meeting the size requirement fall within the scope of the NIS2 Directive. While they are all obliged to fulfill the same legal requirements, not all **are subject to the same supervisory and enforcement measures**.

The Directive classifies the entities falling into its scope into two categories — **essential entities** and **important entities** — each **subject to a different regime**. The categorization is based on how **critical** the entities are to the sector or service they provide, as well as on their **size**.

As a general guidance, the entities belonging to the sectors of high criticality listed in **Annex I** are qualified as **essential entities**, while those belonging to the other critical sectors listed in **Annex II** are qualified as **important entities**.

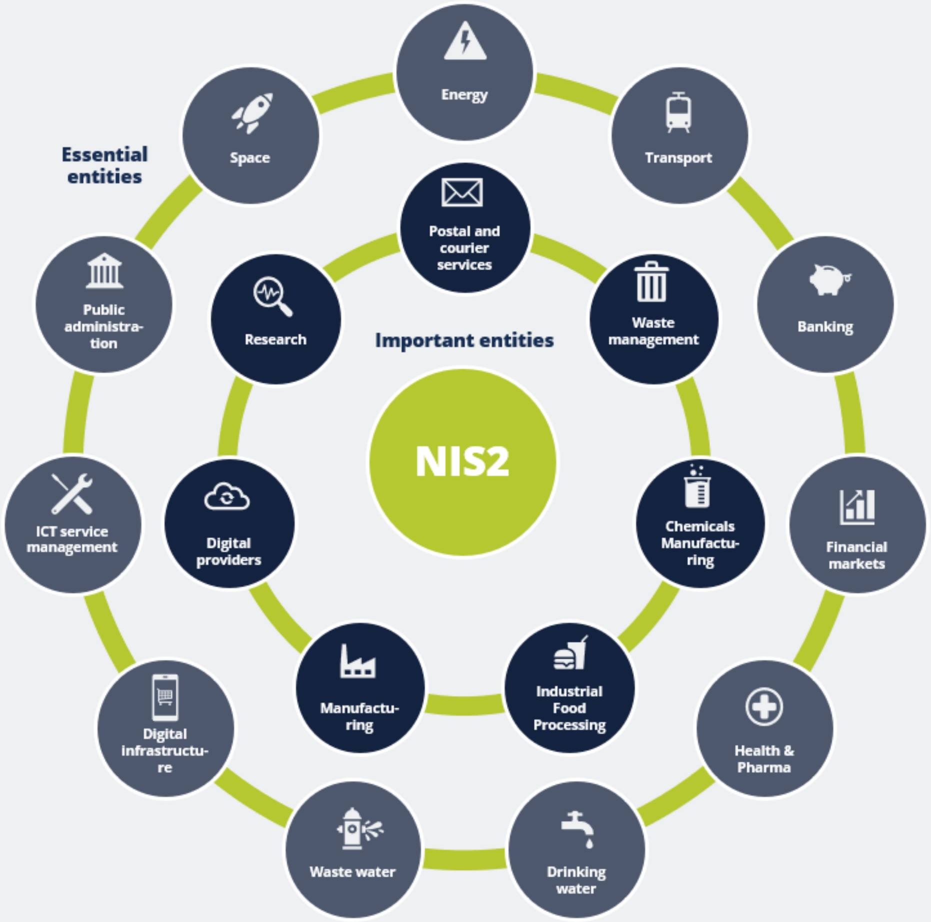
However, an entity belonging to the other critical sectors listed in Annex II is qualified as an essential entity if it is the sole provider in a Member State, or the disruption of its service could have a significant negative impact, or if it has specific importance at a national level.

Where they are listed	Sectors	Entities			Regime they are subject to
		Small < 50 employees/ < € 10Mn turnover	Medium > 50 employees / > € 10Mn turnover	Large > 250 employees / > € 50Mn turnover	
Annex I: Sectors of high criticality	1. Energy (electricity, district heating and cooling, oil, gas and hydrogen);			✓	Essential entities
	2. Transport (air, rail, water, and road);			✓	
	3. Banking;			✓	
	4. Financial market infrastructures;			✓	
	5. Health, including **entities manufacturing pharmaceutical products and preparations, as well as entities manufacturing medical devices considered to be critical during a public health emergency, like vaccines.**			✓	
	6. Drinking water;			✓	
	7. Waste water;			✓	
	8. Digital infrastructure (internet exchange points; cloud computing service providers; data center service providers; content delivery networks;			✓	
	DNS service providers; TLD name registries; trust service providers;			✓	
	Qualified trust service providers and top-level TLD name registries and DNS service providers	✓			
	Providers of public electronic communications networks and publicly available electronic communications services);		✓		
	9. ICT service management: • **managed service providers, providing services related to the installation, management, operation, or maintenance of ICT products, networks, infrastructure, applications, or any other network and information systems via assistance or active administration carried out either on customers' premises or remotely;** • **managed security service provider providing assistance for activities relating to cybersecurity risk management;**			✓	
	10. Public administration;			✓	
	Public administration entity at a national or regional level;	✓			
	11. Space.			✓	
Annex I & II	Entity that is the sole provider of a critical service in a Member State;	✓			
	Entity providing a service whose disruption could have a significant impact on public safety, public security, or public health, or it could induce a significant systemic risk;	✓			
	Entity that is critical because of its specific importance at a national or regional level for the particular sector or type of service;	✓			
	Entity that is qualified as an essential entity by the national legislation implementing the Directive in the corresponding Member State.	Up to the Member State			
Annex II: Other critical sectors	1. Postal and courier services;			✓	Important entities
	2. Waste management;			✓	
	3. Chemicals manufacturing;			✓	
	4. Industrial production, processing, and distribution of food			✓	
	5. Manufacturing of medical devices; computers, electronic, and optical products; electrical equipment; machinery and equipment; motor vehicles, trailers and semi-trailers; other transport equipment;			✓	
	6. Digital providers (online marketplaces, online search engines, and social networking service platforms)			✓	
	7. Research organizations.			✓	

All companies within the scope of the NIS2 Directive are mandated to comply with the same cybersecurity requirements, regardless of whether they are qualified as essential or important entities.

However, **different rules apply to these two categories when it comes to the power given to competent authorities to audit companies and issue fines**.

In essence, essential entities face more proactive and intensive supervision and enforcement measures due to their critical importance, while important entities are subject to similar measures but with a focus on ex-post supervision and slightly less extensive enforcement powers.



The different regime essential and important entities are subject to

Supervisory and enforcement measures:

Essential entities can be subject to on-site and off-site inspections, **regular security audits**, ad hoc audits, and security scans on essential entities to assess their compliance.

Competent authorities have extensive powers to gather information and broad enforcement powers, including issuing warnings, adopting binding instructions, ordering cessation of infringing conduct, imposing fines, and temporarily suspending certifications or authorizations.

Important entities, on the other hand, are only subject to **ex-post supervisory measures**, meaning actions are taken after evidence or indications of non-compliance have been identified or after a security incident has occurred.

The enforcement powers of competent authorities are slightly more limited. They mainly focus on issuing warnings, adopting binding instructions, ordering the cessation of infringing conduct, and imposing fines.

Both essential and important entities are entitled to procedural safeguards, including the right to be informed of preliminary findings, submit observations, and appeal enforcement measures.

Fines and personal liability:

The NIS2 Directive establishes that fines for non-compliance must be effective, proportionate, and dissuasive.

Companies violating the requirements set by the NIS2 Directive can be issued financial penalties - along with enforcement measures, such as warnings, instructions, orders, and so on.

Fines for essential entities can be up to €10,000,000 or 2% of the total worldwide annual turnover, whichever is higher.

For important entities, fines can be up to €7,000,000 or 1.4% of the total worldwide annual turnover, whichever is higher.

If the compliance violation can lead to a personal data breach under GDPR, competent authorities must inform the relevant supervisory authorities, who can impose fines under GDPR for the same conduct.

Additionally, to further strengthen the effectiveness and dissuasiveness of the enforcement measures applicable to **essential entities**, the competent authorities are also empowered to

- temporarily suspend a certification or authorization concerning part or all of the relevant services provided or activities carried out by the entity, and
- temporarily prohibit the Chief Executive Officer or other legal representative from exercising managerial functions. The natural persons holding senior management positions or the power to represent the entity, control it, and take decisions on its behalf (and consequently be able to ensure its compliance) **can be held liable for breach of their duties to ensure compliance** with the NIS2 Directive.

The power given to competent authorities	Essential entities	Important entities
Scope and focus of supervisory measures	• Proactive and random supervision • On-site and off-site inspections, regularly scheduled security audits, ad hoc audits, and security scans. • Competent authorities have extensive powers to gather information and assess compliance ex-ante, regardless of whether an incident has occurred.	Ex-post supervisory measures, meaning actions (after a security incident has occurred).
	Competent authorities can request access to data, documents, and information necessary to carry out their supervisory tasks, as well as request evidence of implementation of cybersecurity policies.	
Enforcement Powers	• Warnings • binding instructions • orders of cessation of infringing conduct • order of informing customers potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures that can be taken in response to that threat; • designation of a monitoring officer to oversee the compliance of the entity • fines • temporary suspension of certifications or authorizations to provide services or carry out activities • temporary prohibition from exercising managerial functions for natural persons • personal liability for breach of duty to ensure compliance with the NIS2 Directive.	• Warnings • binding instructions • orders of cessation of infringing conduct • fines
Financial penalties	Up to €10,000,000 or 2% of the total worldwide annual turnover, whichever is higher.	Up to €7,000,000 or 1.4% of the total worldwide annual turnover, whichever is higher.
Procedural Safeguards	Both essential and important entities are entitled to procedural safeguards, including the right to be informed of preliminary findings, the right to submit observations, and the right to appeal enforcement measures.	

Demystifying NIS2 Requirements

The three areas you should focus your compliance efforts on

secomea

1 **Management's responsibility**

2 **Cybersecurity measures**

3 **Reporting obligations**

Inside NIS2: What are the requirements companies must comply with?

The requirements imposed on companies by the NIS2 Directive can be grouped into three broad areas:

1. Management buy-in, responsibility, training, and liability
2. Preventative measures to mitigate the risk of cyber incidents
3. Reporting obligations in the event that cyber incidents occur

In the following pages, we will analyze each of them in detail.

Management's responsibility for NIS2 compliance

Leadership matters

It can be challenging for businesses to keep up with the latest developments in the cyber landscape, and it can be especially difficult for organizations new to the scope of the Directive to ensure full compliance with all of its requirements.

To make matters worse, companies don't always have the skills and resources to prepare themselves properly. When security experts are not involved in major business decisions, company projects suffer from inadequate safety measures.

Moreover, a **recent study** revealed that 1 in 5 companies believed that **one of the biggest barriers to reducing cyber incidents is the lack of management buy-in.**

Key decision-makers often don't see security implementations as expenses that bring in returns, and that is probably the main reason why security measures are often underfunded.

Board-level action plan to build and practice strong cyber hygiene

Although the subject's complexity cannot be denied, cybersecurity should be considered everyone's responsibility in an organization, not solely of the Chief Information Security Officer.

It is essential that key stakeholders in the C-Suite, such as CEOs, CTOs, CFOs, and other executives, recognize their roles in bringing forth and spreading a strong security culture within the business.

IT and OT security governance should be seen as an integral part of enterprise leadership as it sustains and extends the company's strategies and objectives.

As the role of an organization's leaders is to support their company's mission by ensuring that risks are managed at an acceptable level, cybersecurity needs to be part of the conversation and be kept front of mind to establish a plan of action and investment for the long-term health of the business.

Management is now liable for NIS2 compliance

The EU Commission anticipated that implementing cybersecurity measures required by the NIS2 Directive would entail extensive expenses for obliged organizations. Therefore, it's even more crucial that management is educated in cybersecurity, aware of the risks, and convinced of the need to prioritize it — in this way, the right funding will follow.

The Directive addressed the risk that the C-suite would not devote the appropriate resources to ensure NIS2 compliance by assigning a **company's management the responsibility to approve** the cybersecurity risk-management measures taken to comply with the NIS2 requirements.

Additionally, management is responsible for **overseeing the implementation** of these measures and **can be held personally liable** for compliance failures.

In particular, competent authorities can temporarily remove the CEO or other legal representative from exercising managerial functions in case they find compliance infringements.

Moreover, management is required to follow cybersecurity training and is encouraged to offer similar training to employees on a regular basis so 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.

Management involvement, training, buy-in, and approval of cybersecurity measures are not only a recommended way to proceed — they **are now a legal requirement**. What's more, management is now legally responsible for compliance failures, in which case it can be **suspended from exercising managerial functions**.

1 Management's responsibility

2 Cybersecurity measures

3 Reporting obligations

Cybersecurity risk-management measures listed in Article 21

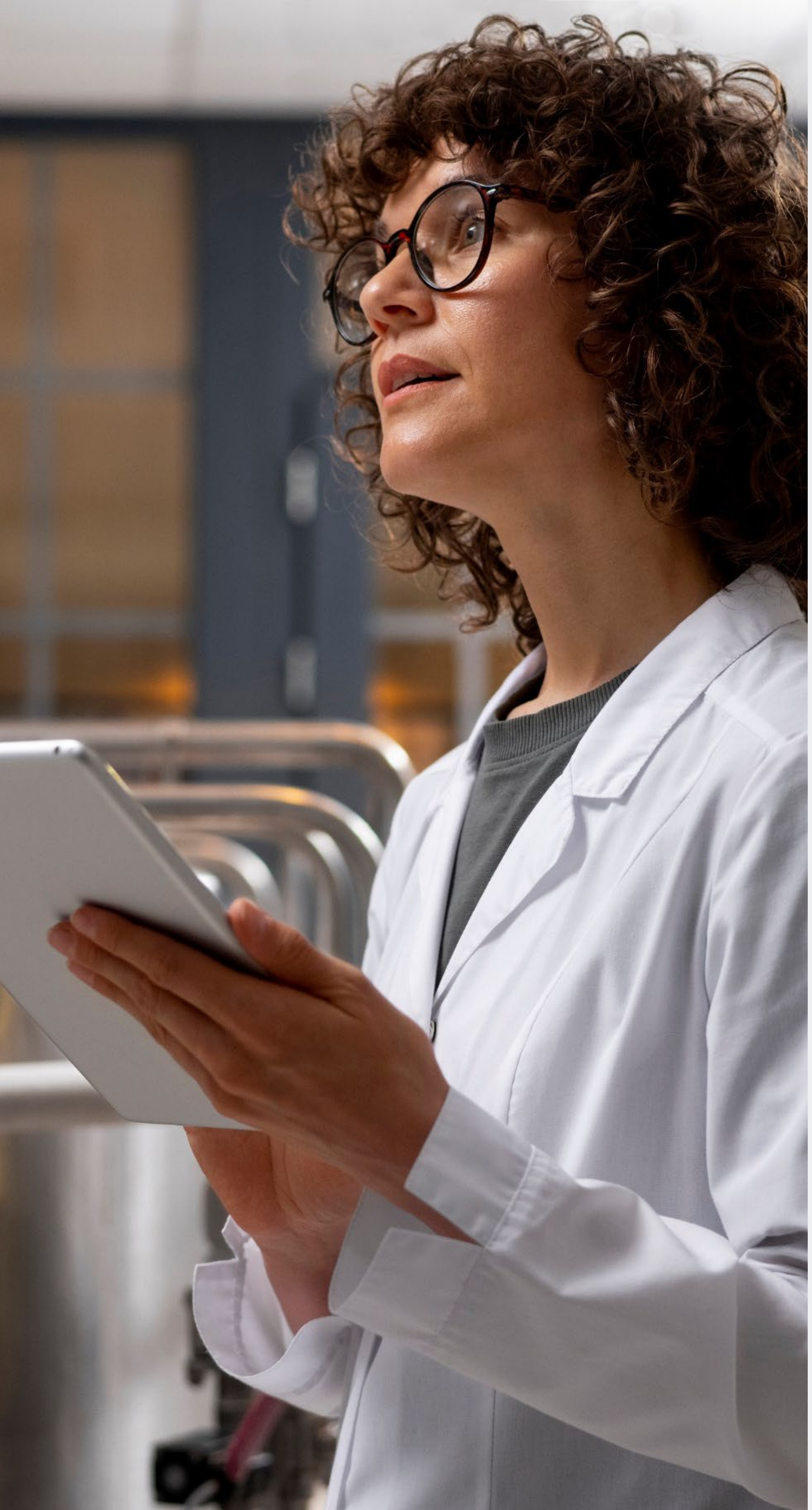
While the NIS2 Directive comprises a total of 46 articles, the one to which companies should devote most of their attention when working toward achieving compliance is Article 21.

Article 21 requires companies to take **appropriate and proportionate technical, operational, and organizational measures** to manage the risks posed to their NIS (network and information system) security and prevent or minimize the impact of incidents on recipients of their services.

Such a statement is meant to broadly include all of the measures necessary to mitigate cyber risks. But what does it really mean?

What are these measures, and how can you make sure they are adequate for your company?

Let's clarify what's intended.



NIS2 requires you to implement

Technical measures

Technical measures are those that can be implemented physically, such as alarm systems, firewalls, cryptography, and encryption. For example, implementing a secure remote access solution like Secomea's to manage and control access to your OT devices and authenticate users via MFA would fall into the category of technical measures implemented under this article.

Operational measures

Operational measures are those related to the processes to follow to proactively ensure cybersecurity and reactively respond in case of an incident. They include how to manage, analyze, and mitigate risks, as well as the steps to take for crisis management or to recover from an incident.

Organizational measures

Organizational measures, on the other hand, are those implemented through instructions, policies, and procedures, such as regular cybersecurity training for staff and, more generally, the focus on building a cyber-secure company culture based on cyber-hygiene practices.

Your cybersecurity measures should be

Appropriate

These measures should ensure a level of security of your network and information systems that is **adequate** to prevent and mitigate the risks posed by potential incidents affecting your NIS security and, in turn, your services – as well as the recipients-users of your services.

In ensuring this appropriate level of security, you should consider the state-of-the-art and relevant international standards, as well as the cost of implementation.

Proportionate

These measures should be **risk-based**: they should take into account your company’s exposure to risks, size, and the likelihood of occurrence of incidents and their severity.

Your risk analysis should be built on an all-hazards approach – meaning that you should consider all of the thinkable threats that could affect your NIS security.

How can you prove to competent authorities that your measures are appropriate and proportionate?

In case of a compliance inspection from the authorities, you must be able to demonstrate that the measures you implemented are appropriate and proportionate. To this end, you will need to be able to prove that:

- The risks and threats you have identified have been handled, the vulnerabilities you encountered in your risk assessment have even been mitigated, and you have been periodically reassessing such risks as well as the effectiveness and adequacy of your measures.
- All 10 minimum requirements listed in Article 21 have been addressed, your incident response plan has been tested, and your company's management has taken an active part in the process and approved it.
- The budget approved by management for cybersecurity is adequate for your company's risk level and size, taking into account the other expenses you have allocated to safety management, for example.
- All of the above is documented, periodically reviewed, and updated as needed.

What exactly should these measures be about? Which elements should they cover?

Your cybersecurity measures should cover, at the minimum, the ten elements listed in Article 21.

If you receive a visit from the competent authorities to audit your organization's compliance with the NIS2 legislation, you need to ensure that you can demonstrate that you have implemented measures, including all of the elements listed below.

Companies violating these requirements will be mandated to take, without undue delay, all necessary, appropriate, and proportionate corrective measures to avoid being issued fines.

10 elements to include in your cybersecurity measures

1. Policies on risk analysis and information system security
2. A plan to be used for handling potential incidents
3. Business continuity, such as backup management, disaster recovery, and crisis management
4. Supply chain security, taking into account the vulnerabilities specific to each direct supplier and service provider.
5. Security in network and information systems acquisition, development, and maintenance - including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
7. Basic cyber hygiene practices and cybersecurity training
8. Policies and procedures regarding the use of cryptography and, where appropriate, encryption
9. Human resources security, access control policies, and asset management
10. 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.

Reporting obligations

Even if you've done everything in your power to prevent a cybersecurity incident from occurring, it can still happen.

Implementing the cybersecurity measures required by the NIS2 Directive will go a long way toward protecting your NIS security and preventing incidents. However, if an incident does happen, you need to be prepared for it and know how to act.

In particular, some reporting obligations need to be attended to. **Companies must notify** their national CSIRT or, where applicable, other competent authorities **without undue delay of any incident that has a significant impact** on the provision of their services.

Let's discover what these reporting obligations entail.

How does the notification duty work?

Which incidents should be notified?

Companies must notify of any incident that significantly impacts the provision of their services.

An incident is to be considered significant if

- it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
- it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Who should be notified?

Companies must notify their national CSIRT (Computer Security Incident Response Teams) or, where applicable, other competent authorities.

Moreover, if the incident is likely to adversely affect the provision of a company's services, the company should also notify its customers (the recipients of the services affected) and, if appropriate, provide information on the cyber threat and the measures or remedies that the recipients can take to respond to it.

Nobody likes to give bad news, but it's your responsibility to reassure the people using your services affected by cyber incidents that you have a best practice plan, that you are working hard to limit the damage, and that competent authorities have been notified promptly.

Despite the crisis, businesses need to be transparent in letting people know when things go wrong: to begin rebuilding trust with your customers, those affected should see you take ownership of the issue and act responsibly in the aftermath.

When should the notification be made?

The notification should be made without undue delay, meaning as soon as possible and, in any case, within 24 hours of becoming aware of the significant incident. In particular, companies must notify authorities:

- within 24 hours, through an early warning indicating whether the incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
- within 72 hours, through an incident notification updating the information shared via the early warning and indicating the initial assessment of the incident, including its severity and impact;
- upon the request, via an intermediate report on relevant status updates;
- within a month after the incident notification, via a final report, including
  - a detailed description of the incident, including its severity and impact;
  - the type of threat or root cause that is likely to have triggered the incident;
  - applied and ongoing mitigation measures;
  - where applicable, the cross-border impact of the incident.

What will happen after a company notifies the authorities of a significant incident?

Upon receiving notification of the incident, the CSIRT will respond to the notifying company within 24 hours, including initial feedback on the significant incident. Companies can also request guidance, operational advice on implementing possible mitigation measures, and even technical support. If the incident is suspected to be of a criminal nature, the CSIRT will also guide the company in reporting it to the competent law enforcement authorities.

Once a company has fulfilled its notification duty, the CSIRT will inform other Member States and ENISA if the cyber incident concerns two or more Member States. If necessary, the incident will also be disclosed to the general public.

These new rules are intended to improve how the EU prevents, handles, and responds to large-scale cybersecurity incidents and crises. They do so by introducing clear responsibilities, appropriate planning, and more EU cooperation to ensure that Member States can mutually assist each other in the case of cross-border malpractices, have a more structured dialogue with the private sector, and coordinate the disclosure of vulnerabilities found in software and hardware sold across the internal market.

4

How to ensure NIS2 compliance

A step-by-step implementation roadmap

secomea

Achieving compliance in practice: how to successfully meet NIS2 standards

When the competent authority comes to audit your organization under NIS2 compliance, they will be expecting you to fulfill a few main objectives:

1. **Risk management**, which includes your processes to properly identify the risks your business runs and demonstrate that management complied with its obligation to be in control and take ownership of this risk assessment.
2. **Protection against cyberattacks**, which consists of the measures you have implemented to limit your exposure to the risks identified and safeguard the cybersecurity of your IT and OT assets and networks.
3. **Detection of cybersecurity events**, which concerns the measures you have implemented to monitor access to your systems—such as user authentication, access management, users' privileges, audit logs, and so on—and to discover potential incidents.
4. **Minimization of cybersecurity events**, which refers to your processes for responding to cybersecurity events, notifying the authorities, and recovering from cyber incidents.

In the following pages, you will find a step-by-step guide to set yourself up for success in your NIS2 compliance program.

10 steps to ensure NIS2 compliance

1 **Assess whether you fall within the scope** of the NIS2 Directive and whether you qualify as an essential or important entity.

2 **Get a good overview of your IT and OT environments and the assets** relevant to providing critical services to society.

An assets audit will give you a better idea of what systems you have, where they are located, who has access to them, and how they are protected. This inventory will give you the knowledge needed to examine the current state of your business's cybersecurity and adequately assess the risks to such assets while considering the threats unique to your business.

Only then you can proceed with threat modeling that best suits your situation. Threat modeling is the process of figuring out what your potential cyber-attacks are likely to be and which operations hackers would be after if they decide to attack you. Where could cybercriminals infiltrate? What would they steal? And finally, how can you prevent it?

Ensure that all the other resources and devices connected to your network whose potential infiltration could spread to the assets that provide critical services are also identified.

3 **Evaluate your risk level.** Your asset inventory will give an initial picture of your cybersecurity status, based on which you can investigate where there is room for improvement and how best to start filling gaps in your defenses.

The identification of your company's specific risks will be your baseline to plan your cybersecurity journey.

When assessing your risks, consider your tolerance level for downtime and map out your priorities for maintaining operations and systems. These considerations will be the foundation for your business continuity, crisis management, and disaster recovery plans (detailed in step 5).

The Directive does not specify who should be responsible for performing the risk assessment in your company. It is up to you to identify the person/s best suited for the job—your cybersecurity team, compliance department, system owners, or similar. What matters (and what the Directive explicitly requires) is that the risk assessment is signed off by management – as management needs to take ownership of the company's risk analysis and risk appetite.

▶▶▶

Pro tip: use Risk Rating best practices

1. **Identify a security risk that needs to be rated:** gather information on the threat agent involved, the type of attack that will be used, and the vulnerability and seriousness of the impact on the business in case of a successful breach, considering the worst-case scenario.
2. **Estimate its likelihood:** understand how likely a particular vulnerability is to be uncovered and exploited by an attacker and generally identify whether the likelihood is low, medium, or high.
3. **Estimate its impact:** calculate the magnitude of a successful attack, both from a technical point of view (interruption of operation, production downtime, data loss) and from a company's perspective (in terms of financial and reputation damage, level of non-compliance exposure, supply chain disruption).
4. **Determine the severity of the risk:** the combination of the likelihood and impact estimates allows you to calculate an overall severity rating for the risk.
5. **Decide how to fix them:** given the risks' classification, create a list of what to fix, generally prioritizing the most severe risks.

10 steps to ensure NIS2 compliance

3.1

Include your supply chain in your risk assessment. For each of your suppliers and service providers, you should collect information on their security, taking into account the vulnerabilities specific to each of them related to their products and services. This is especially important if you rely on critical ICT services, systems, or products, for which it's recommended to use suppliers certified under European cybersecurity certification schemes.

In general, the NIS2 Directive requires you to get to know your supplier by performing some due diligence activities. These activities can help you identify the critical assets your essential services depend on, the cybersecurity processes and practices they have in place, and how they manage vulnerabilities.

Based on these insights, you can assess whether your suppliers can be qualified as NIS2-compliant vendors and classify them based on the quality and resilience of the products they provide.

All this third-party information should then be fed into your risk assessment so that you can assess and describe how to handle the risks entailed and involve management, as they are the ones who need to approve such risk scenarios.

4

Implement the required cybersecurity measures to prevent identified risks, **protect** your IT and OT assets from cybersecurity threats, and **detect** incidents if they occur.

When implementing cybersecurity measures, document the reasons behind your choices.

The Directive requires you to implement cryptography (and, where appropriate, encryption), HR security, access control policies, asset management, multi-factor authentication, etc. However, if you receive a visit from the authorities to inspect your organization, they won't ask you if you configured firewalls and how; they won't look for specific tools and features you have set up in your organization.

They will be looking for indicators of good practice, and they'll be expecting you to let them in on your line of thinking, to be transparent, and to have reasonable explanations for each decision you have made in setting up your defense mechanisms. So, you should be able to demonstrate your reasoning regarding the controls and measures you have or have not implemented.

5

Establish responding modalities to face attacks and **minimize the impact** of cybersecurity incidents. Also, implement processes to **keep potential damage to a minimum and recover the affected operations to ensure business continuity.**

To this end, you should start with an impact analysis: determine which operations are mission-critical or time-sensitive and identify the impact a potential disaster could have on them. This will enable you to properly prioritize the risks and define the order in which the operations should be re-established.

Restoration priorities should be based on criticality: business processes and vital functions with the highest financial and operational impact likely need to be recovered first.

Moreover, you should identify the resources — including both technology and people — that support those mission-critical areas, as well as the resources and stakeholders whose support you'll need to recover operations. During a cyber incident, you should know what assets you need to keep operations running smoothly (people, technology, records, utilities, products), how long it will likely take to restore operations, and who will take charge.

▶▶▶

10 steps to ensure NIS2 compliance

Your crisis plan should involve a coordinated response and avail of the skills of multiple relevant stakeholders across the business (not only your IT and OT teams but also legal, customer service, operations, and anybody who will have to play a role in responding to the incident).

Establish a chain of command with clearly assigned processes and responsibilities to minimize the time from when a disaster hits until the recovery process begins.

6 **Set up procedures to fulfill your reporting obligations promptly** so that, should a cyber incident occur, you can notify the authorities within 24 hours.

Additionally, if needed, inform your customers (the recipients of the services affected) and, if appropriate, provide information on the cyber threat and the measures or remedies they can take to respond to it.

7 **Train your employees to identify risks, detect threats, protect assets, and respond to incidents.** Ensure that all relevant stakeholders are on board and aware of their responsibilities, the actions to perform at each stage, and where to find the answers needed.

8 **Test the effectiveness of your responding modalities.**

A plan cannot be considered complete and in place until there is proof that it will work as expected.

Roles and priorities need to be tested so that you know you can count on the plan when the time comes. So, you should ensure that your employees know what they are supposed to do and that the measures you implemented work as intended.

To this end, it’s recommended to conduct simulated disaster exercises to ensure the effectiveness of the plan and the employees’ readiness.

9 **Ensure your response plans and your overall cybersecurity strategy are up to date.** Running tests periodically, at least once a year, will let you validate your recovery strategies and use lessons learned to make changes or updates if needed.

Additionally, you should ensure that you have taken into account multiple possible incident scenarios, as well as how potential changes in your resources (both technology and people) will affect the effectiveness of your crisis management plan.

For example, will new software or hardware implemented in your IT or OT environments require you to update the existing recovery plan? Are all of the people involved in your response plan still employed at your organization? And if not, have you onboarded somebody else in their role in case of an incident?

Overlooking any of these details could have a serious impact on your cybersecurity preparedness.

10 **Document all of your security measures, controls, and processes within policies** on risk analysis and network and information systems security (in acquisition, development, and maintenance), as well as **plans for incident response,** business continuity, backup management, crisis management, and disaster recovery.

Also, **ensure their appropriate storage** so that they are accessible in time of need.

For instance, consider the risk that the storage location of your recovery plans gets infected. How will you access them, then? Did you do a backup in an alternative cloud?

You could also consider printing them out, which would give you physical safeguards if your whole IT infrastructure is affected.

Tips and easy wins

Regardless of whether you are new to the scope of the Directive, as a manufacturing organization, **there might be some low-hanging fruits you can pick.**

You will likely already have some of the required policies, processes, and measures in place. So, a good starting point could be to review your existing setup with your compliance, QA, and security teams – i.e., analyze your current security program, incident response plan, safety measures, quality assurance program - and, more in general, **the existing controls you have been using** so far - to identify the potential gaps and assess how to move forward.

Besides, you might have been audited before to get an official **certification of compliance with international standards** such as the ISO 9000 family on quality management and assurance, the ISO 27000 series for your Information security management system (ISMS), or IEC 62443 for OT cybersecurity in automation and ICS. Nothing stops you from reusing those existing attestations as a basis for your NIS2 compliance work. Many of the controls and measures included in the mentioned standards can be adapted into the context of the new requirements and be used to demonstrate how you ensure cybersecurity in your IT, OT, and IIoT systems and networks.

Again, as stated earlier, there is no right or wrong framework to use, nor will the authorities ask you about a specific one. What they will want to know is why you have picked a certain control framework over another one, and you should be able to explain the reason behind your choices.

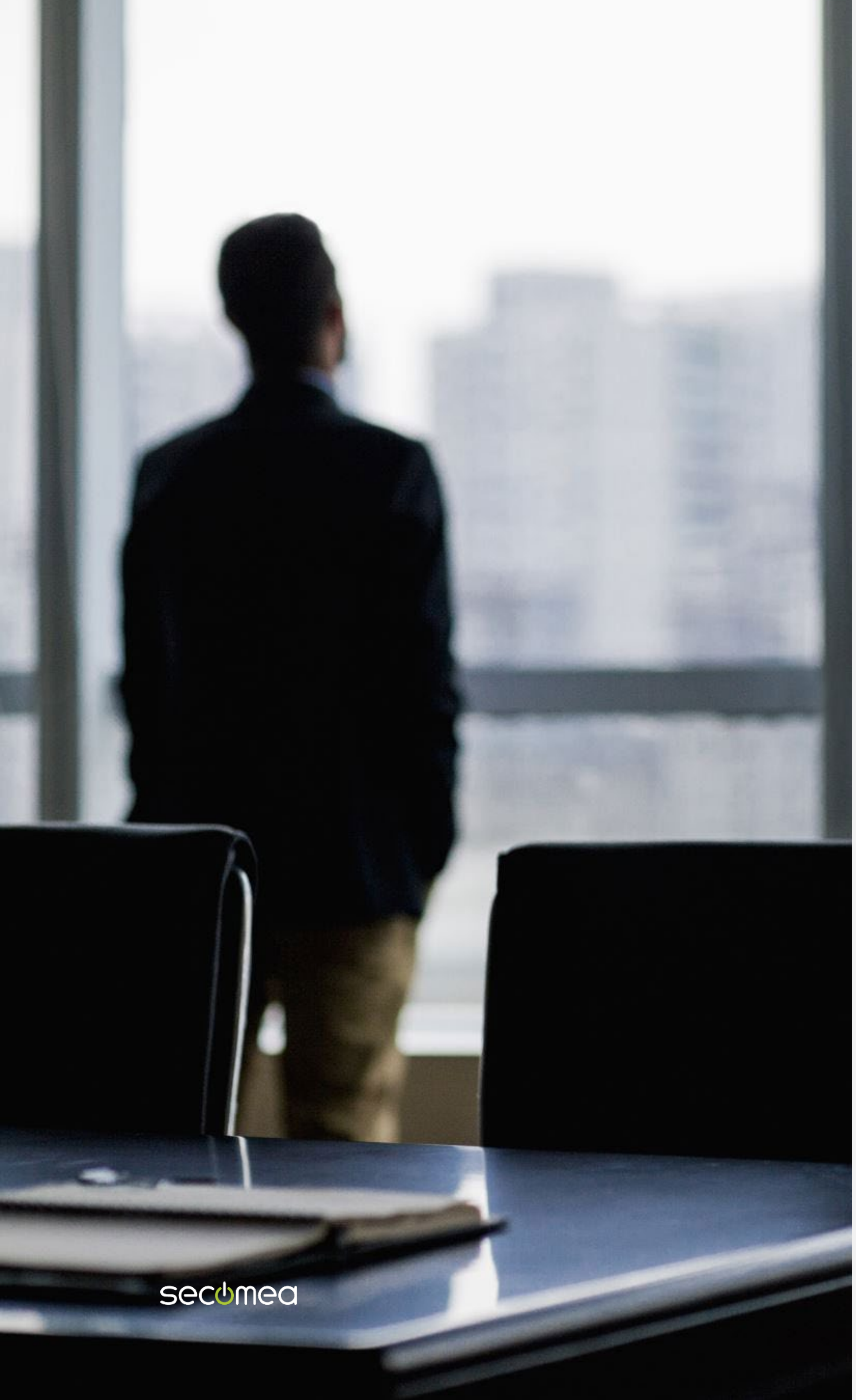
Besides, **if you use Secomea** for your secure remote access needs, you are already off to a great start when it comes to implementing technical cybersecurity measures. If the authorities ask you **how you protect your OT environments**, for instance, you can mention that you chose to implement Secomea precisely because it is purpose-built for OT networks and devices.

Preparing for NIS2 compliance audits

Best practices and success strategies

5

secomea



What if the authorities come knocking on your door? Get ready for NIS2 inspections

If your organization falls within the scope of the NIS2 Directive, you should prepare for the possibility of being visited by the authorities.

If you are an essential entity, you will be subject to regularly scheduled inspections planned randomly, regardless of whether an incident has occurred. You will typically receive a letter from the competent authority about two weeks before the scheduled audit date informing you of the upcoming inspection (and perhaps the specific subject areas they will investigate).

If you are an important entity, you will only be inspected ex-post—i.e., after an incident has occurred.

Regardless of whether your organization qualifies as an essential or important entity, **you can take some relevant actions to prepare for the inspection** and support its positive outcome.

Tips for a successful NIS2 compliance audit

Before the inspection

During the inspection

After the inspection

- ✓ First, you should **inform management and the relevant internal business units** of the upcoming audit and its nature, scope, and date.
- ✓ Then, you should **form a team** of those who will be responsible for preparing for and participating in this cybersecurity audit.
- ✓ These people should be **appropriately trained** to be aware of their role in this upcoming inspection. Moreover, you might want **to ensure the availability of additional subject matter experts** on the inspection date so that you can involve them should the competent authority wish to discuss their specific areas of responsibility in more detail.
- ✓ Finally, **perform a gap analysis** by reviewing your documents and **looking for possible deficiencies**. If you identify areas in need of improvement, take the necessary measures to do so. If it’s not feasible to fully correct such deficiencies before the inspection date, prepare descriptive documentation of the issues you encountered and the actions you have taken to address them.

Tips for a successful NIS2 compliance audit

Before the inspection
During the inspection
After the inspection

- ✓ On the date of the inspection, it's advisable **to agree upfront on the duration of the audit, its scope, and the agenda for the day** to ensure alignment and agreement on how to proceed.
- ✓ **Prepare a short and concise presentation to introduce your company** and the nature of your business to the competent authority. That's the first step in helping them understand whether the cybersecurity measures you implemented are appropriate and proportionate to your organization—and, ultimately, whether you are meeting the NIS2 Directive requirements or not.
  - The presentation should show that you have identified the services critical to society that you provide, the assets needed to provide them, the measures implemented to protect them, the vendors you rely on for the provision of your services, the customer segments using your services, and the delivery channels through which you provide them. To help you do that successfully, our Compliance Manager at Secomea prepared **a template including all these elements. You can download it here** and update it with your company information. If you present the competent authorities with such an overview, you'll be up to a great start and give a positive first impression. Besides using it as part of your compliance documentation in case of an inspection, you could also rely on it as an excellent instrument to kick off your internal NIS2 compliance project.
- ✓ **Make sure to have at hand all of the documentation you have prepared to present during the audit.**
  - This documentation should show how you assess risks, detect threats, protect assets, and respond to incidents – as well as prove the involvement of C-level management in all of your decisions.
  - If you have picked an international security framework to adhere to, provide documentation on it, as that represents a structured approach to work with security and is a good way to show progress.
  - If your gap analysis revealed deficiencies, provide documentation about their identification and your plan to address them.

Tips for a successful NIS2 compliance audit

Before the inspection

During the inspection

After the inspection

The inspection outcome will vary depending on your preparedness and NIS2 compliance level. When exercising their enforcement powers, competent authorities will consider the particular circumstances of each case, such as the nature, gravity, and duration of the infringement, the damage caused or losses incurred, and the intentional or negligent character of the infringement.

Authorities' findings	Consequences
There is no trace of NIS2 being known within your organization: You have completely ignored the enforcement of the NIS2 Directive.	You will likely be issued heavy fines.
You have done the bare minimum: You might have implemented just a few cybersecurity measures, but your overall risk assessment and risk management strategy are still behind in achieving full NIS2 compliance.	You will probably be issued fines proportionate to your infringements and given a deadline to implement the necessary improvements.
You have tried to achieve compliance to the best of your ability, but deficiencies have been uncovered	The authorities will likely not issue a fine but engage in a dialogue with you to instruct you on the areas needing improvement, and they will establish a deadline for you to implement such improvements. If that happens, make sure to put in place the required measures within the set deadline to avoid the issuance of fines.
You have followed all the necessary steps and implemented best practices	If the authorities assess that you are following industry standards and thoroughly fulfilling the NIS2 objectives and requirements, the audit will be successful.

Secomea: your trusted partner for NIS2 compliance

Security, solutions, and features
to support your NIS2 readiness

6

NIS2 compliance made easy, with Secomea

Concrete examples of how can we help you in your NIS2 journey

The implementation of Secomea's secure remote access solution on your factory floors can be qualified as one of the technical measures that you are required to take under Article 21 of the NIS2 Directive to manage the risks posed to the security of network and information systems and prevent or minimize the impact of incidents.

Additionally, using Secomea will address the following elements mandated by the legislation:

NIS2 requires you to:

- **Implement access control policies and asset management:**

  Managing and controlling access to your assets is precisely what Secomea is for.

  With Secomea, you can

  - ✓ provide access to defined assets
  - ✓ handle role-based access permissions for each of your users and each of your assets
  - ✓ provide access to users after they have requested it
  - ✓ provide access to users for a defined timespan

- **Implement Multi-Factor Authentication:**

  With Secomea, you can

  - ✓ enable Multi-Factor Authentication using
    - ○ SMS Authentication
    - ○ Single-Sign-On (SSO) via OpenID Connect
      - ○ Microsoft Azure Active Directory (Azure AD)
      - ○ Okta

- **Have a plan in place to handle incidents and ensure business continuity (crisis management and disaster recovery):**

  Secomea enables you to connect (and disconnect) machines to your network. This means that should a problem arise—e.g., a cyber-attack infecting one or more of your devices—you can use Secomea to cut that machine's access to your network, thereby preventing viruses or malware from spreading to other machines.

  Therefore, Secomea is an essential tool for handling incidents and a crucial component in your organization's business continuity, crisis management, and disaster recovery plan.

  With Secomea, you can

  - ✓ access audit logs to review remote access sessions. Should an incident occur during a remote access session, you will be able to access an audit log detailing who accessed the affected device, when, and for how long. This will help you identify the cause of the incident and mitigate it.
  - ✓ set-up up alerts, events, SMS/email alarms, and automated actions to get notifications of specific events related to your machines' status
  - ✓ prevent risks when downloading files on your machines by using the "secure file transfer" feature; the feature ensures all files transferred to and from an engineering station are scanned for viruses or malware before they are accessible to the user.
  - ✓ access the Vulnerability Hub to assess your overall vulnerability score based on the risks you run due to outdated firmware on SiteManagers and identify the necessary actions to prevent downtime. For each SiteManager in every one of your sites, get notified if you need to update its firmware to the latest version or replace hardware that has reached End of Support.

NIS2 requirements	Secomea's features that help you address it
Access control policies and asset management	✓ Network management and customization to your company's internal policies ✓ Appliances access management ✓ User access management ✓ User and asset control ✓ Request for access
Multi-Factor Authentication	✓ 2FA & MFA ✓ SMS Authentication ✓ Single-Sign-On (SSO) • Microsoft Entra ID (Azure AD) • Okta
Incident handling and business continuity	✓ Audit logs ✓ Alerts, events, SMS/email alarms, and automated actions ✓ Data Collection Module ✓ Secure file transfer ✓ Vulnerability Hub

Let's not forget: NIS2 requires you to ensure supply chain security – and Secomea can support you in doing that

Secomea's contribution in helping you assess the risks posed by your suppliers is two-fold:

✓ **As a secure supplier:**

In providing you with our secure remote access solution, Secomea represents one of your suppliers whose risks and vulnerabilities you need to assess under the NIS2 Directive.

At Secomea, security is our top priority. The following pages will offer an overview of our risk management and cybersecurity practices, demonstrated by our third-party certifications.

✓ **As a guarantee of security of the other suppliers you rely on who use Secomea:**

As the leading provider of secure remote access solutions for OT networks and appliances, Secomea is widely used worldwide by over 9,500 manufacturing organizations and machine suppliers. Therefore, standardizing remote access for all stakeholders in this ecosystem is integral to our company mission.

This also means that, when assessing the risks posed by your suppliers, you will likely find that many of them use Secomea as well, which gives you assurance on the security of their remote access processes – and, in turn, saves you time in rating their risk level.

Building trust: Secomea’s commitment to ensure security every step of the way

At Secomea, cybersecurity takes up a pivotal role.

Everything we do follows internationally recognized industry best practices, and each stage of product development meets rigorous cybersecurity standards.

As a result, our products can be trusted to be secure from the moment they are deployed and after updates and new features are released.

Security is not only part of product development. It’s deeply rooted in our company culture.

Cyber-hygiene practices involve all aspects of our business, from R&D to sales, customer service, marketing, and operations – as well as the external partners and distributors who represent us globally.

Our security certifications

To show our formal commitment to securing our services, our system continually undergoes third-party security audits and assessments.

Through this significant investment, Secomea ensures the most advanced protection for its customers and demonstrates compliance with the following industry standards and best practices:

- **IEC 62443:** IEC 62443 is an international series of standards specifying process and functional requirements for the secure development of products used in industrial automation and control systems (IACS). In particular, we have been audited for:
  - **IEC 62443-4-1 on secure product development lifecycle requirements:** this certification confirms that Secomea develops and maintains secure products by following a secure development lifecycle (SDL), including a secure-by-design development methodology, secure implementation, patch management, and product end-of-life.
  - **IEC 62443-3-3 on system security requirements and security levels:** this certification attests to Secomea's compliance with the technical control System Requirements (SRs) associated with the seven foundational requirements (FRs): Identification and authentication control (IAC), Use control (UC), System integrity (SI), Data confidentiality (DC), Restricted data flow (RDF), Timely response to events (TRE), and Resource availability (RA).
- **ISAE 3402**: Our organizational security measures are assessed and documented in a third-party ISAE 3402 report, which is the international standard providing assurance on an organization's adequate internal controls.

  Our certification attests that our controls are consistent, complete, repeatable, and auditable and demonstrates to our customers that they are adequate to ensure the security of Secomea's services.

  Secomea's controls have been reviewed based on the guidelines specified in **ISO 27002** for organizational information security standards and information security management practices.

Our security is your security

How we ensure the security of Secomea's products

Secomea is using the following practices:

- **Specification of security requirements**

  Minimum security requirements for the products' development and deployment are established.

  Threat analysis and risk assessment play important roles in identifying and classifying potential security risks. They involve defining trust boundaries for process, data, and control flow, including any communication to internal and external peripherals.

- **Secure by design**

  Our products are designed to implement the security principles of dependability, trustworthiness, and resilience.

  We ensure they are secure by design through the application of best practice principles such as defense in depth and threat modeling.

- **Security verification and validation testing**

  We verify the security of our products before deployment through validation testing that demonstrates the products' defense-in-depth strategy is effective.

  We apply a requirements-based testing approach to show that functional and security requirements have been correctly implemented.

Secomea is an official CVE Numbering Authority (CNA)

Secomea has been formally recognized by the Cybersecurity & Infrastructure Security Agency (CISA) as a CVE Numbering Authority (CNA) . This means the CVE Program has authorized us to assign CVE IDs to vulnerabilities and publish CVE Records. In other words, Secomea is one of the 364 entities worldwide that can identify and name cybersecurity vulnerabilities—the first (and, until very recently, the only) one in Denmark.

Therefore, we have a **Cybersecurity Advisory Process** in place through which our customers can report suspected security vulnerabilities they have discovered. Our support team will evaluate the validity of the suspicions, and - if vulnerabilities are identified - our R&D department will address them through product updates to remediate and mitigate the risks that have arisen. The reporter will be notified, and the vulnerabilities will be disclosed to the CVE list.

Our official identification as a CVE Numbering Authority (CNA) is further proof of the paramount importance we give to security. Thanks to it, we are not only able to identify and respond to vulnerabilities and work with customers to mitigate their risks. We are also enabled to be transparent and show our customers that we keep ourselves accountable for the security of our products and, in turn, their operations.

Together, we make manufacturing the most secure industry in the world.

secomea

About Secomea: How we help you defend your factory floor

Offices in Denmark (HQ), US, China, Japan

Represented in 35 countries through our 70+ Distributors, Alliance Partners and OEM Partners

+9.500 customers, over 300.000 SiteManagers installed in thousands of production sites worldwide

Secomea Highlights

Manage remote access in a few clicks

Plug-and-play for ICS: PLC, HMI, SCADA

High security by design

Purpose-built for OT equipment

Global reach, local support

Easy to use for you and for your technicians

Implementation at record speed

Supports all protocols: RDP, VNC, SSH, Telnet

New platform built on a zero-trust architecture

Secomea products overview: your turnkey IIoT platform

Why Secomea is trusted by over 9.500 manufacturers and machine builders worldwide since 2008

Secomea is a Secure Remote Access (SRA) solution purpose-built for industrial networks and OT equipment. We simplify OT remote access so you can have global oversight while maintaining local control.

Our turnkey IIoT solution includes all software and hardware components needed for performing your remote access and maintenance tasks – from remote programming and troubleshooting to data-driven decision-making.

Our brand-new platform built on a zero-trust architecture, **Secomea Prime**, gives you complete oversight over your remote access sessions.

The **SiteManager IIoT Gateway** is the key component of the solution, which, in combination with the **GateManager IIoT Server** and **LinkManager Access Client**, connects you transparently to machines anywhere in the world.

Secomea Prime

Achieve full control of your remote access sessions

SiteManager IIoT Gateway

Easily connect our hardware to any OT device (or install the software version)

GateManager IIoT Server

Drag and drop: Seamlessly manage user access to appliances

LinkManager Access Clients

Authorized users can access the appliances from their browser

secomea

secomea.com