10 steps to ensure NIS2 compliance

A practical checklist for critical infrastructure and manufacturing organizations

SECOMEA

01 DOES NIS2 APPLY TO YOU?

YES ☐ NO ☐

Confirm you're in scope

Check whether your organization qualifies as an "essential" or "important" entity under NIS2 – based on your sector and size.

Does your company have

- ○ more than 50 employees **or**
- ○ over €10 million in annual turnover?

and

- ○ operate in one of the sectors listed on the right?

Important entities

- *Research*
- *Waste management*
- *Manufacturing*
- *Digital services*
- *Postal and courier services*
- *Industrial food processing*
- *Chemicals manufacturing*

Essential entities

- *Energy*
- *Transport*
- *Banking*
- *Financial markets*
- *Health & Pharma*
- *Drinking water*
- *Waste water*
- *Digital infrastructure*
- *ICT service management*
- *Public administration*
- *Space*

02 HAVE YOU APPOINTED A RESPONSIBLE PERSON OR TEAM?

YES ☐ NO ☐

Identify stakeholders that can support you within your organization

Assign a team or leader with clear accountability for NIS2 compliance, including reporting and governance responsibilities.

03 DOES LEADERSHIP UNDERSTAND THEIR NIS2 OBLIGATIONS?

YES ☐ NO ☐

Involve management

Ensure your executive team is aware of their role in compliance and their potential liability under NIS2.

04 ARE YOU AWARE OF YOUR RISK LEVEL?

YES ☐ NO ☐

Conduct a risk assessment

Map your critical assets and assess risks – including third-party risks – to understand what needs to be protected.

Make an inventory of your assets

- ○ What resources do you use to provide critical services?
- ○ What systems are employed?
- ○ Where are they located?
- ○ Who has access to them?
- ○ How are they protected?

Evaluate your risk level

- ○ What risks are you subject to?
- ○ Which operations would hackers be after if they decide to attack you?
- ○ What would they steal?
- ○ Where would hackers try to infiltrate your network?
- ○ What are their potential cyber-attacks likely to be (malware, phishing, etc.)?
- ○ What are the most serious vulnerabilities you should prioritize (based on their likelihood of occurring and impact severity)?
- ○ How can you prevent them?

04.1

ARE YOUR VENDORS NIS2-COMPLIANT?

YES ☐ NO ☐

Perform supply chain due diligence

Your supply chain should be included in your risk assessment to evaluate your suppliers' security level and confirm you can identify them as NIS2-compliant vendors.

- How do your suppliers ensure security?
- What cybersecurity processes and practices do they have in place to protect the products and services they provide?
- How do they manage security vulnerabilities?
- Do they hold third-party security certifications?
- Can you qualify them as NIS2-compliant vendors?

05

DO YOU HAVE APPROPRIATE AND PROPORTIONATE CYBERSECURITY MEASURES IN PLACE?

YES ☐ NO ☐

Implement technical, operational, and organizational controls

These measures are listed under Article 21 of the Directive and include MFA, secure remote access, backup procedures, and network segmentation.

- Have you setup MFA as an identity verification method to access your IT and OT assets?
- Do you have policies on risk analysis and information system security?
- Do you have a plan for handling potential incidents?
- Have you addressed your supply chain due diligence duties?
- Have you set up processes to handle vulnerabilities and disclose them, if necessary?
- Do you regularly test the effectiveness of your cybersecurity risk-management measures?
- Do you provide your employees with cybersecurity training?
- Do you use cryptography and encryption to protect your data?
- Have you set up access control policies?

06

DO YOU HAVE A DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN?

YES ☐ NO ☐

Define your cybersecurity strategy

Develop a plan to detect, report, and recover from security incidents quickly and effectively.

- Which operations are mission-critical or time-sensitive, and which resources (both technology and people) support those mission-critical areas?
- What impact could a potential cyber incident have on those operations?
- In the event of an incident, who will take charge?
- Which operations should be re-established first?
- Which departments will be involved?
- What will the chain of command look like?
- How will you minimize the time from when a disaster hits until the recovery process begins?
- How will you minimize the impact of a cybersecurity incident?
- How will you keep potential damage to a minimum?
- How will you recover the affected operations to ensure business continuity?

07 HAVE YOU SET UP A PROCESS TO TIMELY NOTIFY AUTHORITIES OF SIGNIFICANT INCIDENTS?

YES ☐ NO ☐

Prepare for reporting obligations

Know when and how to notify authorities (e.g., CSIRTs) within NIS2's required timeframes for major incidents.

- Do you have a process in place to fulfill your reporting obligations promptly?
- Does the process enable you to notify the authorities within 24 hours, follow up with an update within 72 hours, and prepare final report within one month?

08 ARE YOUR EMPLOYEES ABLE TO IDENTIFY RISKS, DETECT THREATS, AND RESPOND TO INCIDENTS?

YES ☐ NO ☐

Train staff and raise awareness

Provide regular cybersecurity training and ensure all employees — not just IT — understand their responsibilities.

- Are they aware of the actions they should perform in the event of a cyber incident?
- Do they know where to find the answers they need?

09 HAVE YOU TESTED THE EFFECTIVENESS OF YOUR RESPONDING MODALITIES?

YES ☐ NO ☐

Periodically test, review, and update your response

- Have you tested roles and priorities to ensure that your employees know what they are supposed to do?
- Have you tested that the measures you implemented work as intended?
- Have you conducted simulated disaster exercises to ensure the effectiveness of the plan and the employees' readiness?
- Have you taken into account multiple possible incident scenarios?
- Have you considered how potential changes in your resources (both technology and people) will affect the effectiveness of your crisis management plan?
- Does your response plan need to be updated to address these changes?

10 CAN YOU PROVIDE DOCUMENTATION DETAILING YOUR APPROACH TO CYBERSECURITY?

YES ☐ NO ☐

Document all your NIS2 compliance activities

Keep detailed records of your controls, policies, risk assessments, and response plans — this will be critical during an audit.

- Have you documented all of your security measures, controls, and processes within policies?
- How do you ensure their appropriate storage so that they are accessible in time of need?
- Have you created any backups?