EXPERT PAPER

Expert Paper

Introduction to NIS2 and impacts on private enterprise

Autobahn security

Executive summary

The Network and Information Security Directive 2 (NIS2) is a critical regulation for enterprises operating in the European Union (EU). Obligations for organizations to adhere to these new regulations will take effect at the end of 2024.

The NIS2 directive extends the scope of its predecessor, NIS1, and imposes stricter security requirements on entities that provide essential services or operate digital platforms.

Whereas NIS1 had six sectors, 12 additional sectors are now being added to NIS2 — for a total of 18 sectors with compliance obligations.

This expert paper discusses the three main areas of focus for Chief Information Security Officers (CISOs) and security leaders as they develop their compliance action plan for NIS2.

About Autobahn Security

Autobahn Security is a SaaS platform that saves IT security professionals time — and empowers IT teams to make their networks more secure.

Our platform aggregates, filters and prioritizes vulnerabilities from multiple scanners and turns them into easy-to-understand remediation guides.

Autobahn Security is the result of decades of white-hat hacking and security consulting experience for Fortune 500 companies. Autobahn Security is trusted by companies across multiple industries in over 20 countries, including Allianz, SwissPost and Taboola.

Key takeaways

There are three questions CISOs need to ask: is my organisation impacted, are there interactions with existing legislation, and does my board know what this entails?

1. CISOs should determine if their organization is affected by NIS2 by identifying if they are an Essential Entity (EE) or an Important Entity (IE). Additionally, CISOs should determine if their entity size makes them regulated under NIS2, as the directive concerns only medium and large companies.

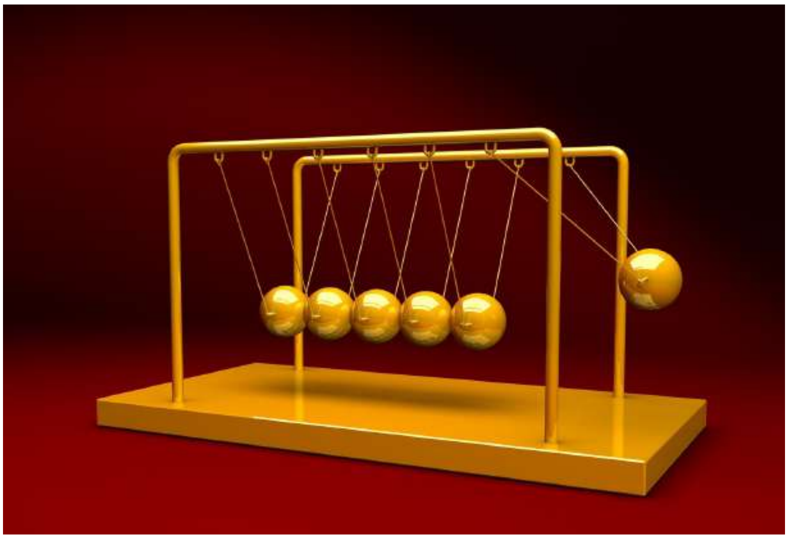
2. For companies operating in industries where there are other cybersecurity rules, they should figure out how these rules work together with NIS2. For instance, for energy companies, the Risk Preparedness Regulation should be understood as a complement to NIS2, and for financial companies, the Digital Operational Resilience Act (DORA) is considered more specifically important than NIS2 — and where there is a perceived conflict between the two wordings, security professionals should defer to the DORA.

3. CISOs should raise awareness among senior management about the potential sanctions and fines for non-compliance with NIS2. The NIS2 directive introduces the notion of top management accountability for security, and the CEO and Board of Directors must be aware of the latest news and what to do to ensure better governance. Essential Entities face administrative fines of up to €10 million or 2% of annual worldwide turnover, and C-level executives may be held liable for cybersecurity risk management.

At a glance

	NIS1	NIS2
Scope	Applies to DSPs (Digital Services Providers) and OESs (Operators of Essential Services)	Redefined to cover Essential Entities (EE) and Important Entities (IE)
Company Size	Nothing specified	Concept of entity size: 'micro' and 'small' enterprises are exempt
Reporting obligations	Voluntary	Mandatory
Incident notification deadline	No deadline specified	24 hours
Penalties for non-compliance	Determined by member states	Harmonized across the EU with maximum penalties of 2% of annual turnover or €10 million (whichever is higher)
Cooperation and information sharing	Encouraged but not mandatory	Mandatory for designated CSIRTs (Computer Security Incident Response Teams) and incident response teams in case of cross-border incidents, pan-EU operators
Security requirements	General obligation to implement appropriate technical and organizational measures	Specific security obligations based on risk assessments and sector-specific standards
Supervision and enforcement	Member states responsible for enforcement	Designated national competent authorities responsible for enforcement
Supply chain security	No actions specified	Entities should perform due diligence of their supply chain

So, am I impacted?



For its scope, the NIS2 directive distinguishes two types of entities:

- Essential Entities (EE), detailed in Annex I of the NIS2 text
- Important Entities (IE), detailed in Annex II of the NIS2 text

The **Essential Entities (EE)** cover the following sectors:

- Energy
- Transport
- Banking
- Financial market infrastructure
- Health
- Drinking water
- Waste water
- Digital infrastructure – cloud providers, data centers, DNS, etc.
- ICT service management (B2B): Managed service providers and Managed Security Service Providers
- Public administration
- Space

The **Important Entities (IE)** cover the following sectors:

- Postal and courier services;
- Waste management;
- Manufacture, production and distribution of chemicals;
- Food production, processing and distribution;
- Manufacturing of:
- medical devices and in vitro diagnostic medical devices
- computer, electronic and optical products
- electrical equipment
- machinery and equipment.
- motor vehicles, trailers and semi-trailers
- other transport equipment

Digital providers of:

- online marketplaces
- online search engines
- social networking services platform
- Research organizations

Company size and exceptions

The NIS2 directive only impacts medium and large companies. Headcount and financial limits determine these categories:

- SMEs have <250 employees and annual turnover ≤EUR 50m OR annual balance sheet total ≤EUR 43m.

However, the following entities are covered by the directive regardless of size:

- Public electronic communications networks or publicly available electronic communications services
- trust service providers
- TLD name registries and DNS service providers;
- public administration entities;
- central government entities, as defined by a Member State;
- Regional government entities as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities.
- Sole providers of a service in a Member State;
    - a potential disruption of the service provided by the entity could have an impact on public safety, public security or public health;
    - a potential disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;
    - the entity is critical because of its specific importance at regional or national level for the particular sector or type of service, or for other interdependent sectors in the Member State;
    - the entity is identified as a critical one under Directive (EU) 2022/2557 – aka the Critical Entities Resilience Directive (CER).

The NIS2 states that each Member State shall establish a list of the national entities covered by the above points.

Where to begin?

Incident reporting: Compliance with the NIS2 directive requires organizations to establish a framework for reporting cyber incidents that significantly impact operations, finances, or physical harm to relevant authorities and customers.

Covered organizations must file an initial report within 24 hours of a significant incident, followed by a more detailed report within 72 hours, and a final comprehensive report within one month. CISOs should ensure that their organization has the necessary reporting capabilities to meet these requirements.

Risk management and liability: NIS2 imposes stricter risk management measures on regulated entities. Organizations must have policies on risk analysis, incident handling, supply chain security, vulnerability management, encryption, security awareness training, access management, multi-factor authentication, and other areas.

These policies must be ratified by the highest governing body of the organization to boost internal transparency of cyber risks and mitigations. The directive assigns accountability for cybersecurity and compliance to senior management, which could lead to personal liability for negligence or non-compliance. CISOs should work closely with their organization's senior management to develop and implement policies that meet NIS2 requirements.

Vulnerability management: NIS2 makes vulnerability management and supply chain security core risk management responsibilities for regulated entities and their managers.

CISOs should ensure that their organization has a comprehensive vulnerability management plan in place and consider partnering with providers that can assist with monitoring for vulnerabilities and implementing security patches.

Your NIS2 preparedness survey

Ask leadership, your organization (and yourself) these questions to see what the current state of play is.

1. Does your organization operate in a designated sector as defined by the NIS2 Directive? (Energy, transport, water, banking, financial market infrastructures, healthcare, and digital infrastructure)

2. Are you aware of the NIS2 Directive and its requirements for businesses in designated sectors?

3. Has your organization conducted a comprehensive risk assessment to identify its cybersecurity risks?

4. Does your organization have a cybersecurity strategy that includes policies, procedures, and controls to mitigate cybersecurity risks?

5. Does your organization have a designated cybersecurity officer and a cross-functional cybersecurity team?

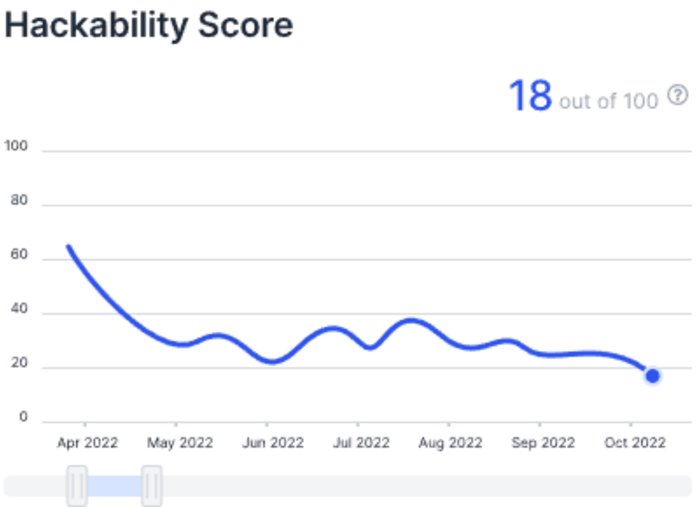
6. Does your organization have communication and training programs to ensure that employees and stakeholders are aware of their cybersecurity responsibilities and the risks associated with cybersecurity incidents?

7. Does your organization have a cybersecurity incident response plan that outlines the steps to be taken in the event of a cybersecurity incident (detection, containment, and recovery)?

NIS2 compliance cheatsheet

Task	Description	Status	Notes
Conduct Risk Assessment	Identify potential threats and vulnerabilities to systems		
Establish Security Measures	Develop a plan to mitigate risks and improve security measures		
Implement Access Controls	Limit access to critical systems and data		
Create Incident Response Plan	Establish clear policies and procedures for incident reporting and communication with authorities		
Appoint Point of Contact	Designate a point of contact for communication with authorities in the event of a cyber incident		
Regularly Review and Update Security Measures	Ensure that security measures are effective against new and evolving cyber threats		
Test Incident Response Plan	Test the incident response plan to ensure it is effective and employees are aware of procedures		
Train Employees	Provide cybersecurity training to all employees to ensure they are aware of risks and their responsibilities		

How Autobahn Security can help



Under NIS2, vulnerability management is a critical responsibility for regulated entities and their managers.

The directive requires organizations to develop policies on vulnerability management and implement measures to reduce risk.

By working with Autobahn Security you can optimize your vulnerability scanning, prioritize vulnerabilities based on their severity, and receive clear remediation guidance that can help your organization comply with these requirements.

Additionally, our Hackability Score provides a common language to communicate your security posture to board level or other departments.

Having a single comprehensive KPI to measure security simplifies reporting — and provides certainty to non-security experts that are nonetheless accountable under the new regulations.

Fortune 500 companies are already working with Autobahn Security to quickly identify and prioritize vulnerabilities — helping their organizations identify potential attack vectors and mitigate them before they can be exploited, reducing the risk of a significant incident.

NIS2 next steps overview

Some key recommendations for businesses to improve their NIS2 compliance and preparedness include:

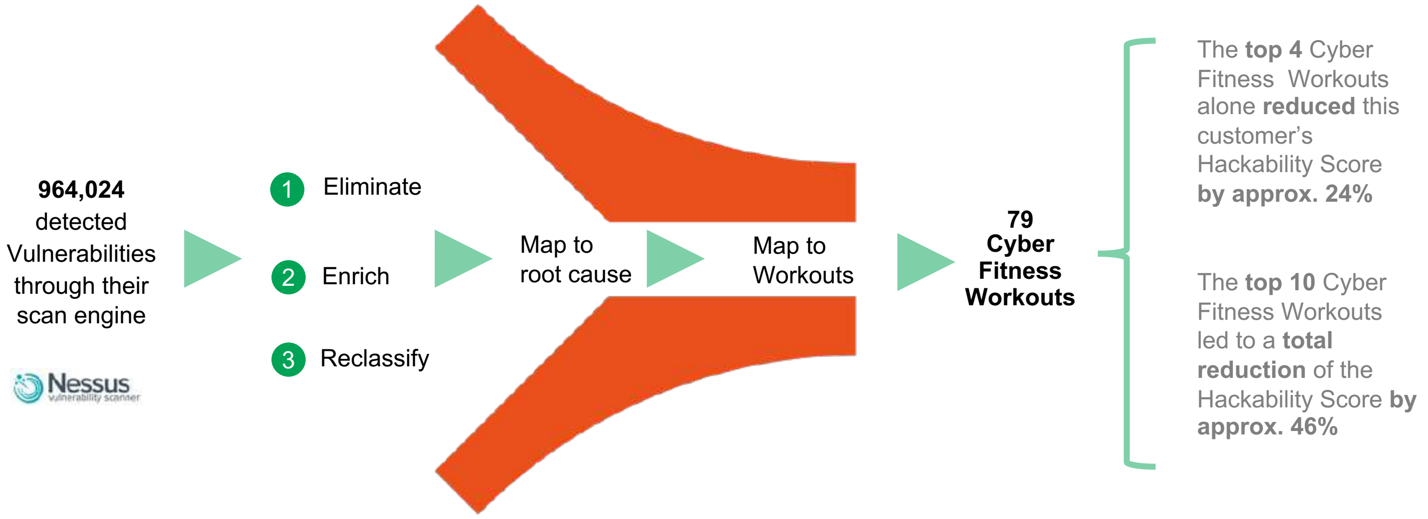
- Conduct a cybersecurity risk assessment to identify and prioritize critical assets and systems, and implement appropriate security controls to mitigate risks.
- Develop a comprehensive incident response plan that outlines procedures for detecting, reporting, and responding to cybersecurity incidents, and ensure that employees are trained on the plan.
- Implement best practices for cybersecurity such as using strong and unique passwords, multi-factor authentication, and regular software updates and patches.
- Maintain situational awareness of cybersecurity risks and threats through regular threat assessments and intelligence gathering, and ensure that the entire organization is informed of any emerging risks.
- Regularly review and update cybersecurity policies and procedures, and ensure that they are aligned with the NIS2 directive and any other relevant regulations.
- Foster a culture of cybersecurity awareness and accountability throughout the organization, and ensure that all employees are trained on basic cybersecurity hygiene and best practices.

Conclusion

CISOs should establish an incident management system that includes policies, procedures, and training to ensure that employees understand and comply with security requirements. Enterprises that operate essential services should conduct regular cybersecurity assessments to identify and remediate vulnerabilities.

CISOs should adopt a risk-based approach to cybersecurity, which involves identifying, assessing, and mitigating risks to their operations. Enterprises should establish a security management system that includes risk assessment, security measures, and incident management. Organizations must also report significant incidents to national authorities, which will share information with other member states.

How Autobahn Security works



964,024 detected Vulnerabilities through their scan engine

1. Eliminate
2. Enrich
3. Reclassify

Map to root cause

Map to Workouts

79 Cyber Fitness Workouts

The **top 4** Cyber Fitness Workouts alone **reduced** this customer’s Hackability Score **by approx. 24%**

The **top 10** Cyber Fitness Workouts led to a **total reduction** of the Hackability Score **by approx. 46%**

A Comprehensive Guide to Implementing a Vulnerability Management Process

Book a free expert call

Expert Paper

How to get started — and what you can expect in Week 1

01. Getting to know the key aspects of Autobahn Security's SaaS platform

02. Understanding your pain points and issue remediation processes

03. Learning how to set up vulnerability scans

04. Evaluating scan results and start remediating

Request your free expert cybersecurity consultation right now

In your individual tailored discussion, an Autobahn Security expert will evaluate your individual challenges, provide a product overview, explain our value process and discuss potential milestones and next steps.

You can also benefit from a free all-access trial of the software, with no obligation.

Talk to a member of our team to see how Autobahn Security can help make your organisation Cyber Fit

Book a free expert call