infinigate
spark your growth

NIS2, it's all about ensuring your business continuity.

Start now and achieve compliance in small, manageable steps.

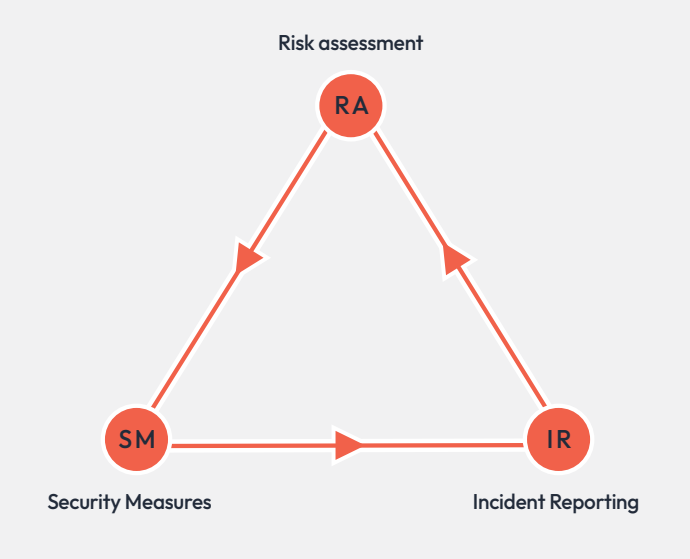
Introduction

No doubt, you have heard of NIS2. So why have most people never heard of NIS1, its precursor? NIS1, the first EU-generated cybersecurity-focussed directive, issued in 2018, was focussed on national authorities rather than companies, aiming to harmonise cybersecurity regulations across the EU member states.

NIS2, first introduced in 2022, brings the directive to a wider business level, as every member state of the EU is required to translate the directive into legal requirements for business by October 2024.

It focuses on two key areas: security measures, to prevent cyber breaches and prepare your company to respond effectively in case of an incident on the one hand, and incident reporting, if the worst happens, on the other. It mandates legal requirements for cybersecurity risk management and for incident reporting.

The inspiring principle for both NIS1 and NIS2 is one and the same: it is all about resilience, to keep your business running, unimpeded by cybersecurity incidents and cyber-threat disruption; for the EU, this equates to keep the economy safe from costly interruptions.



Following NIS2 recommendations is in your business interest, to ensure its continuity. You can look at it as a kind of partnership between national authorities and infrastructure owners.

Compliance with the NIS2 directive means your business is able to detect and respond quickly to a cyber incident, handle a crisis situation and keep your services running through a business continuity plan.

The NIS1 and NIS2 directives imply an ongoing process, rather than something you do just once. It starts with risk assessment based on asset and inventory recording, progressing to security measures and incident reporting, if your business is impacted by a breach. It is a cyclical process of continuous monitoring, prevention and reporting.

Who must adhere to the NIS2 directive?

NIS2 imposes stricter legal requirements for cybersecurity for hundreds of thousands of European companies. Although NIS2 is a directive at EU level, each country will issue specific regulations based on its baseline requirements. They will become a legal requirement for companies of a certain size in critical sectors. The critical sectors listed under the NIS2 directive are: energy, health, finance, transport, drinking water, digital infrastructure, digital service providers, electronic trust services and electronic communications. You can find them listed here: https://nis2directive.eu/who-are-affected-by-nis2/

infinigate
spark your growth

Where do I start on the route to NIS2 compliance?

There are some key steps to systematically approach NIS2 compliance, treating it as a gradual journey, without being phased by the complexity of the guidelines. You cannot compress this journey into a few days, so start well ahead of time.

Type of organisations impacted by NIS2

Medium entities: ≥50 FTE and ≥€10m turnover

Large entities: ≥250 FTE and ≥€50m turnover

Across 11 essential and 7 important sectors

1 Are you impacted?

Look at the criteria of the type of organisations who must comply with the regulations. You may want to follow the regulations anyway, as your business will benefit from them.

2 Align your internal stakeholders.

Identify experts and owners of critical data and infrastructure elements.
Ensure your C-suite is participating.

3 Risk assessment.

Identify you risk areas and level. Where do your key data and assets reside?
How vulnerable are they to being intercepted? What would happen if a breach occurred?
Don't forget your production and supply chain!

4 Set up a crisis management plan.

In case of a breach, do you have a process to follow, to avoid delays and costly interruptions to your services?

5 Incident reporting process.

Do you have a list of actions for reporting a cybersecurity incident, with clear ownership and contacts?

If you are already ISO 27001 or IEC 62443 certified, the good news is that you'll be very well-positioned to meet the requirements of the NIS2 Directive, with about 70% of the requirements covered. But beware of that 30% gap (see comparison table below).

The new EU directive extends the requirements for risk, asset management and business continuity plans. It also requires companies to put in place standardised incident reporting processes.

It imposes personal liability on executive management. This means that they will need to be more involved in security processes than before and will therefore need to receive appropriate training.

	ISO27001	NIS 2
Transparency & passing due diligence (audits and inspection by authorities →	**Data Discovery** **Documentation**	
Structured path to operationalise compliance & keeping up-to-date →	**Recommendations** **News**	
Awareness & education employees →	**Academy/Awareness Training** **Policies/Templates** (NIS2: also mandatory for exec. management)	
Manage risk →	**InfoSec/Cybersecurity Risk Management** (NIS2: even more emphasis & depth)	
Single source of truth for your partners / vendor management →	**Supply Chain Security** **Procurement Security**	
Build trust with your customers & upside →	**Reporting to Authorities** (NIS2:<24h) **Incident Response** **Management Approval Process**	
Resource Management →	**Asset Management** **Backup Management**	

In conclusion, we recommend starting early and taking a pragmatic, systematic approach to NIS2, remembering that your effort will pay off in terms of business continuity.

Your local IT reseller should be able to advise you on potential solutions to help you plug any cybersecurity gaps in your organisation, ensuring that your existing infrastructure is interoperable and compliant.

NIS2 Compliance Checklist

- ☑ **Understand Applicability**
  Determine if your organisation falls under the categories of essential or important entities as defined by NIS2. Review the list of sectors and subsectors affected by NIS2, including energy, manufacturing, transport, banking, digital infrastructure, public administration, and more.
- ☑ **Governance and Risk Management**
  Establish a governance framework to manage cybersecurity risks. Identify and document all information systems and digital infrastructure.
- ☑ **Security Measures**
  Implement technical and organisational measures to ensure the security of network and information systems. Ensure measures are in place for incident prevention, detection, and response.
- ☑ **Incident Reporting**
  Establish an incident reporting mechanism in line with NIS2 requirements. Train staff on identifying and reporting incidents. Report significant incidents to the relevant national authority within the stipulated timeframe.

For NIS2 related queries, please contact:

Patrick Scholl, Head of Operational Technology at Infinigate, on patrick.scholl@infinigate.de