

# Navigating NIS2: A guide to European cybersecurity regulations

# The evolution of cybersecurity regulations in Europe

The changing role of cybersecurity regulations in Europe reflects the growing recognition of the increased threat that breaches and cybercriminals pose to individual companies and organisations — and to society more broadly. Because our society is now made up of ever-more interlinked organisations, any attack can have wide-ranging and unexpected consequences.

Recent changes to European Union (EU) regulations, known as NIS2 (Network and Information Security Directive 2), also mention the impact of COVID-19 on working practices. With more of us working from home since the pandemic, the potential threat surface increases, as does our reliance on networks to get work — and the rest of our lives — done.

But it also reflects the growing maturity of cybersecurity regulation. While organisations work to stay secure there is also recognition that we need unified laws and minimum standards to keep us all safe.

The first step in this journey was taken in 2016, with the Network and Information Security Directive, or NIS1. This established basic cybersecurity standards for organisations working in critical sectors including water, digital infrastructure, banking, healthcare and transport. NIS2 expands on these, embracing a much wider pool of sectors.

Having said that, it should be noted that NIS2 is a directive not a law — it needs to be passed into national law by member states, which some states have already done. NIS2 is now in effect, with several countries, including Belgium, Croatia and Italy, incorporating it into local law and others in the process of adopting it.

NIS2 is transforming and informing regulation both within the EU and beyond. This is another key driver of cybersecurity legislation. It does not operate in a single nation-state. Companies that interact with citizens or other companies in the EU are expected to follow the same rules. We're moving towards a world where cybersecurity standards are shared across countries, and companies will be obliged to comply to do business and to reassure customers that they are implementing regulations.

It should also be noted that the UK government has pledged not to adopt NIS2 into national legislation, but instead to extend NIS1 in line with other regulations, such as the Cyber Security and Resilience Bill. But looking at what is actually suggested, it appears that the UK and EU are moving in the same direction with the changes being made — although the proposed UK legislation promises to be less onerous. When the UK government will find parliamentary time to make these changes is also unclear. In reality, most organisations working or trading with the EU will likely choose one set of rules to comply with rather than two.

# The basics of NIS2

## Who:

Applies across the EU, but companies anywhere in the world doing business with, or providing services to, companies or organisations within the EU will also have to follow NIS2 practices.

Extends rules from large organisations dealing with critical infrastructure to smaller companies and those defined by the EU as essential.

Rules extended to companies with more than 50 staff in certain sectors.

Energy, transport, banking, health, digital infrastructure, cloud computing providers, managed security service providers, waste management, food producers, large parts of manufacturing industry, search engines and research bodies are all included.

## What:

Sets rules for countries to be prepared for cybersecurity incidents and encourages cross-border cooperation.

Member states were supposed to transpose the directive into national law by October 2024. Several have done so, while others are in various stages of adoption. Check the [current state of transposition](#).

Compulsory incident notification.

## How:

Cybersecurity is a clear responsibility of senior management — and NIS2 does this by making them personally responsible for failures.

The directive, and its national law equivalents, covers a wider selection of companies and organisations — not just vital infrastructure, but those defined by the EU as essential.

Defines a duty to give early warning of incidents within 24 hours and provide more detailed notification in 72 hours and a detailed report within a month. This aims to create two beneficial effects. Firstly, to encourage compliance under threat of unwelcome publicity and, secondly, to provide actionable insights for other organisations likely to be targeted by similar attacks.


# NIS2 essentials: What you need to do to comply

It should be noted that NIS2 reads very much like any ‘best practice’ handbook for good, general cybersecurity hygiene, albeit one that comes with tough financial penalties for failure. Sanctions under NIS2 are tough, with fines of up to €10 million or 2% of annual global turnover, whichever is higher.

Compliance with the directive and protection for the business means determining what is needed to protect devices, assets and data. This means physical security, cybersecurity and staff trained to operate securely. In addition to implementing such measures, organisations must also demonstrate that they have an effective risk management strategy in place. That includes proving what you’ve done — that you’ve assessed the state of your networks, IT systems and human skills, and acted where appropriate.

You need to show that you have a plan in place for incident handling if the worst does happen. You will need to demonstrate that you have evaluated supply chain security, vulnerability handling and disclosure — and that you have a strategy in place for the use of cryptography and, where appropriate, encryption.

NIS2 recognises EU cybersecurity certifications of products and solutions to help ease the compliance burden on businesses. If your organisation is already ISO 27001 compliant, you are well on your way to satisfying NIS2.

A background image showing a person's hands writing on a document with a pen. The image is dark and slightly blurred, focusing on the hands and the pen. The text is overlaid on the left side of the image.

But, as always, compliance should not be seen only as an end in itself. Compliance can be a great way to win hearts and minds and to get broad backing for cybersecurity strategies that should be part of business thinking at every level anyway. Compliance does not mean complete protection, but it certainly won't put you at more risk.

Most organisations now understand that they need to plan for incidents — even as they hope that these never occur and work hard to stop them ever happening.

Equally, the mood has changed on incident reporting. More people now accept the benefits and the role that incident reporting plays in keeping other organisations safer, and they recognise that it even provides a blueprint for defending against new attacks.

# Best practices for compliance and security: Understanding the difference

Cybersecurity professionals need to understand the difference between achieving compliance and achieving best possible protection. These are not the same thing. Organisations need to demonstrate compliance — you need to be able to show, with evidence, to a third party that what you have done is as secure as possible. It's like showing your insurance company that you've got the right locks and alarms in place to secure your warehouse. That is all necessary, but you need to go beyond that to be truly secure.

**Here are 13 elements to consider in your journey to NIS2 compliance:**



**Network security policy:** Establish a policy on the security of network and information systems that sets forth the roles and responsibilities of the various departments of the business with a process to monitor compliance.



**Risk assessment:** Establish and implement an incident handling policy setting forth the roles, responsibilities, and procedures for detecting, analysing, containing or responding to, recovering from, documenting and reporting of incidents in a timely manner.



**Business continuity and crisis management:** Develop and maintain a business continuity, crisis management and disaster recovery plan to apply in the case of cybersecurity incidents and other crises that includes back-up plans for critical resources, including personnel. Train applicable personnel on these documents and conduct regular simulated crises to make sure everyone knows and can perform their roles.



**Supply chain security policy:** Create and implement a supply chain security policy that includes an assessment of potential suppliers' security practices as part of the contracting process.



**Understand use of information and communication technology (ICT) vendors:** Map your ICT vendors, what they do, which ones are critical to your operations, and the security standards these vendors must meet. Maintain a directory of critical suppliers, including contact information. Develop a process to assess vendor compliance with the security standards.



**Cyber risk process assessment:** Create a process in which you assess the effectiveness of your cyber risk procedures and perform that assessment periodically.



**Security training:** Provide cybersecurity training and promote basic cyber hygiene practices among employees to foster a culture of security and awareness.



**Cryptography:** Develop and enforce the correct use of cryptography and encryption to ensure the confidentiality and integrity of sensitive data.



**HR security:** Implement policies and procedures that govern employee behaviour regarding cyber security hygiene. Use appropriate background screening procedures in compliance with applicable law when hiring personnel. Create a standard process to revoke all access to the company's information technology assets and company information when employees leave the company.



**Access control:** Implement security procedures for employees with access to confidential data. Use multifactor authentication (MFA) and continuous Zero Trust evaluation, and where appropriate, encrypt internal emergency communications to improve security measures.



**Classify company assets:** Set up a system to classify company information, such as business confidential information and sensitive information (e.g., health information, government ID numbers, credit cards, etc.).



**Environmental and physical security:** Evaluate supporting critical infrastructure for company sites, such as communications systems and power, and where feasible, implement back-up processes. Protect physical locations from outside threats, including physical access controls.

# People and processes first, technology second

Vendors are often guilty of selling solutions first. But in reality, you need to start by putting in place the right processes, procedures and people, and then think about technology to support and strengthen these capabilities. Security teams often regard humans as the weakest link rather than their first line of defence.

Training your staff and enhancing their security skills is a vital step — and one recognised in the NIS2 directive.

Any regulatory change is a good opportunity to revisit the basics and assess what you are doing well and where there is room for improvement.

You need good access controls and identity management. You need email protection — still the most common vector and starting point for an attack. You need network protection and firewalls too.

But you also need some more intelligent security systems working for you. Looking at network and application behaviour is increasingly important in a world where identifying the ‘edge’ of any network is getting harder every day. This can also help protect you from supply chain attacks.

Barracuda can help you meet NIS2 requirements — and improve your overall security posture — with application protection, network protection and email protection. We can even provide managed XDR to oversee it all.

# About Barracuda

Barracuda is a leading global cybersecurity company providing complete protection against complex threats for all sized businesses. Our AI-powered BarracudaONE platform secures email, data, applications, and networks with innovative solutions, managed XDR and a centralised dashboard to maximise protection and strengthen cyber resilience. Trusted by hundreds of thousands of IT professionals and managed service providers worldwide, Barracuda delivers powerful defences that are easy to buy, deploy and use. For more information, visit [barracuda.com](https://barracuda.com).

