GETTING STARTED WITH NIS 2

YOUR GUIDE TO A FAST, SUSTAINABLE PATH TO MANAGING COMPLIANCE

isms.online

What is the NIS 2 directive?

Network and Information Security (NIS 2) is the European Union's directive that aims to improve a common level of security for network and information systems and thereby strengthen cybersecurity across the EU.

The NIS 2 directive will bring providers of outsourced IT and managed service providers within the scope of the rules to better protect essential supply chains and critical national services from cyberattacks.

In this guide, we've summarised some of the fundamental changes to the NIS 2 directive to help organisations identify the key areas they need to review to comply with the regulations.

What are the core requirements of the NIS 2?

NIS 2 will require organisations to ensure the following measures are in place to manage cybersecurity risks:

INFORMATION SECURITY POLICY

A critical part of cybersecurity is assessing your risk level. NIS 2 will require companies to evaluate the potential impact of an attack on their most vital assets and be alert to potential network vulnerabilities or news of other industry members being attacked. They will also need to take a proactive rather than reactive approach to risk management by introducing strong information security policies to ensure systematic and thorough risk analysis.

INCIDENT PREVENTION, DETECTION, AND RESPONSE

NIS 2 requires organisations to have plans and backup plans, run drills and train all relevant parties. Once an organisation has identified their most significant vulnerabilities, the updated directive requires them to implement clear procedures to prevent attacks and agree on methods to detect potential incidents. This should result in an incident response plan with a transparent chain of command for implementation.

BUSINESS CONTINUITY AND CRISIS MANAGEMENT

The updated NIS 2 intends to ensure that a business can continue its operations in the event of a cyberattack. Organisations must have a verifiable plan for how the company will react to an attack and how it can recover from it as quickly as possible, minimising disruption. As a result, NIS 2 includes a focus on cloud backup solutions.

SUPPLY CHAIN SECURITY

Supply chain security has been under the microscope globally for some time. NIS 2 doubles down on this and requires organisations to consider the vulnerabilities of each of their suppliers and service providers and their cybersecurity practices, including data storage providers. The directive ensures that organisations clearly understand the risks, maintain a close relationship with suppliers, and continually update security to guarantee the highest possible protections.

VULNERABILITY DISCLOSURE

NIS 2 will require more transparent vulnerability disclosure and management. Organisations must provide ways for the public to report any vulnerabilities and ensure the relevant department acts upon this information. If an organisation identifies a vulnerability within their network, the updated directive requires them to disclose it. Disclosure of such vulnerabilities will support the fight against cybercrime and ensure they are not exploited elsewhere.

INCIDENT REPORTING

Under the updated directive, companies must submit an initial report within 24 hours of becoming aware of any “significant” incident, a full incident notification within 72 hours and a final report within one month to any relevant competent authority, Computer Security Incident Response Team (CSIRT), and sometimes, to their customers.

A “significant” incident is any incident that has caused or is capable of causing severe operational disruption of the service or financial losses or if the incident has affected or is capable of causing considerable losses to others.

COLLABORATION

The first NIS directive failed because it did not consider the different ways individual countries operated. Therefore NIS 2 will:

- **Encourage more data sharing between authorities**
- **Require authorities to participate in incident response at the EU level rather than national**
- **Establish an EU-Cyber Crisis Liaison Organisation Network (EU CyCLONe), a central body to coordinate and manage responses to EU-wide cyber incident**s

By centralising cybersecurity controls at the EU level and mandating that everyone adheres to the same cybersecurity standards, NIS 2 aims to simplify a previously under-coordinated system. This should facilitate collaborative data sharing and more efficient solutions to cyber incidents as they occur.

Who needs to comply with NIS 2?

NIS 2 will apply to any organisation with more than 50 employees whose annual turnover exceeds €10 million and any organisation previously included in the original NIS directive

The updated directive will also increase its scope to include the following new industries:

Industries included in the original directive will remain within the remit of the updated NIS 2 directive.

What are the implications of not complying with NIS 2?

NIS 2 comes with much stricter enforcement requirements than its predecessor. Penalties for nonconformity range from being security audited and ordered to follow set recommendations to fines of €10 million or 2% of the organisation's total worldwide turnover – whichever of these numbers are higher.

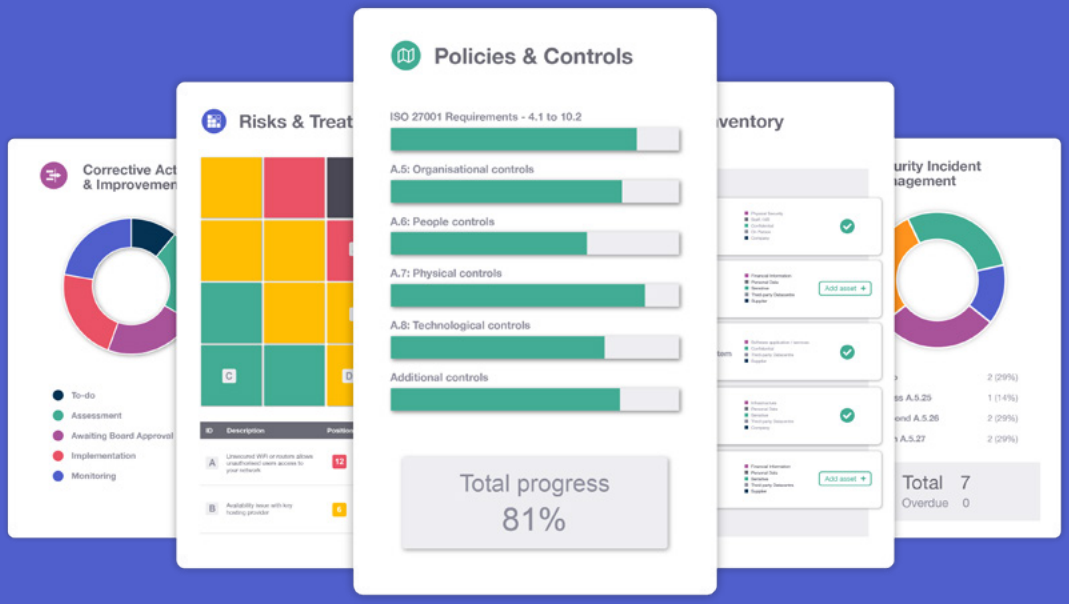
Notably, these fines are the same as those imposed for GDPR violations, and NIS 2 should be understood similarly. The NIS 2 initiative represents a significant leap in cybersecurity and should be treated as seriously as the considerable sea change GDPR drove for data protection.

How to comply with the NIS 2 regulations?

For organisations looking to achieve compliance with NIS 2, certification against ISO 27001 could be a decisive first step.

ISO 27001 can help organisations meet NIS 2 requirements while achieving independently accredited certification. This provides evidence to suppliers, stakeholders and regulators that you have taken the appropriate and proportional technical measures required and demonstrate a competitive edge within the marketplace.

An ISO 27001-compliant information management system (ISMS) enables organisations to reduce their risk and exposure to security threats by identifying the relevant policies they need to document, the technologies to protect themselves and the staff training to avoid mistakes. They also mandate that organisations conduct annual risk assessments, which helps them stay ahead of the ever-changing risk landscape.



The ISMS.online solution

ISMS.online brings alive the security principles required for the NIS 2 Regulations.

Achieving NIS 2 compliance through ISO 27001 is a very effective way of managing risks associated with information security threats within an organisation. Our cloud-based platform comes pre-configured with tools, frameworks, policies and controls, actionable documentation, and guidance to meet every ISO 27001 requirement in a secure, shared workspace. It makes creating an ISO 27001 ISMS a simple, speedy task.

DASHBOARD

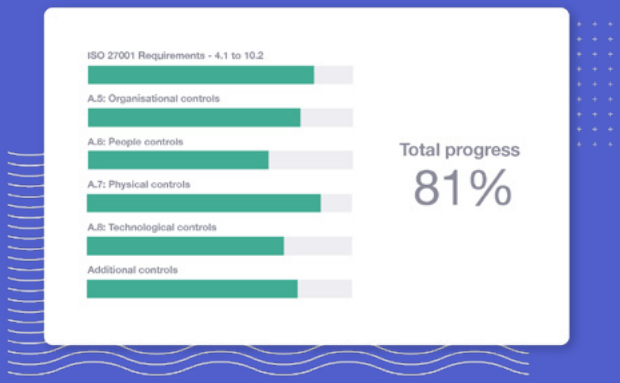
One dashboard, all risks

ISMS.online acts as a single source of truth by reducing risk gaps or duplications across multiple systems. Linking the NIS 2 Regulations and ISO 27001 is easy in ISMS.online and will prevent duplication of the many requirements and speed up implementation.

POPULAR STANDARDS

Supporting over 50 standards and regulations

With control mapping, the platform provides easy access to any compliance framework, standard or regulation, including the ability to create custom ones. Beyond NIS 2 and ISO 27001, ISMS.online users can utilise our platform to achieve other standards and regulations, including ISO 27701, ISO 22301, GDPR, SOC 2, HIPAA and many more.



HEADSTART

Save time

With Headstart, the journey to ISO 27001 is 81% complete from the moment you first log in. You can adopt the pre-configured content, adapt anything you need and then add any specific policies and controls to fit your business.

- **81% of the work done for you**
- **No need to build policies from scratch**
- **Save hours on your ISO 27001 project**

HELP & SUPPORT

Support whenever you need it

No need to wait for help. Get your answers straight away with Virtual Coach – your always-on-guide to ISO 27001 certification or from our experienced Customer Support team.

- **Always on support from Virtual Coach**
- **Experienced Customer Support team**
- **Extra help available from our in-house specialists**

INTEGRATIONS

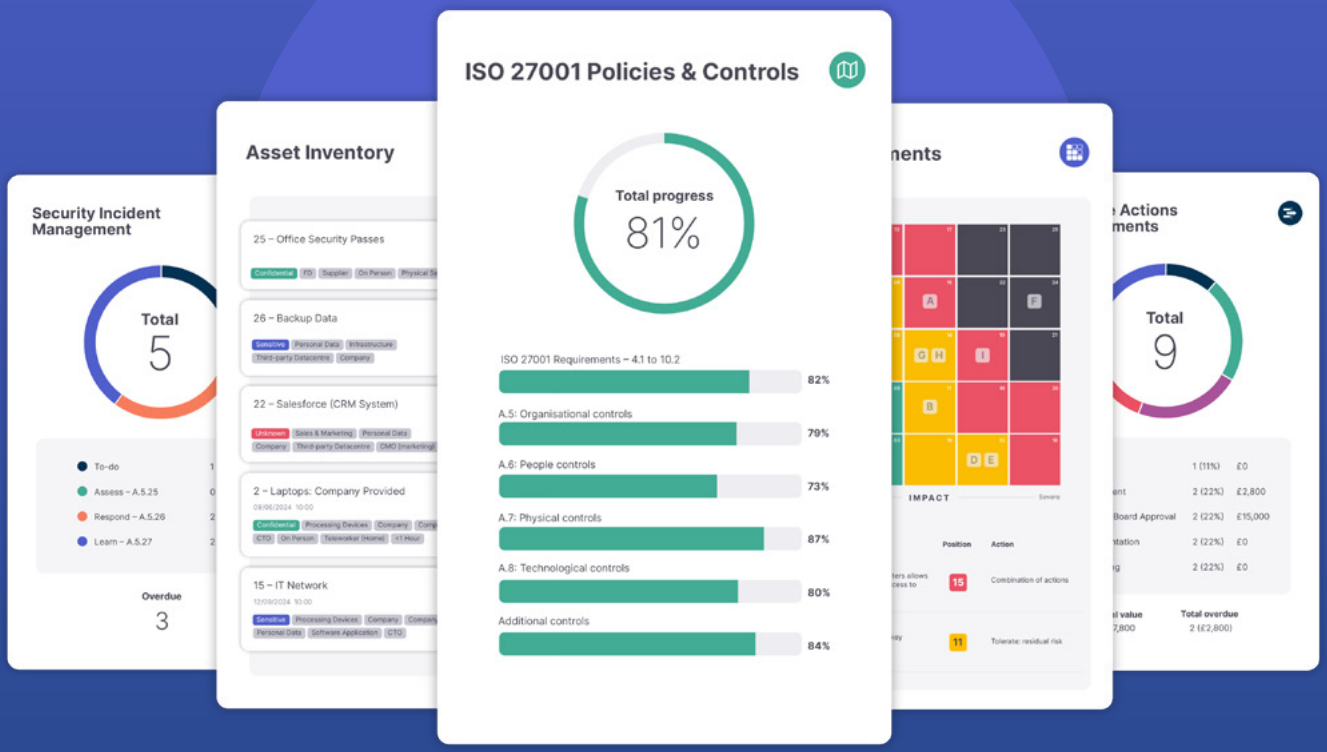
Works with your existing systems

ISMS.online works with your existing systems, so there is no need to double your workload. Integrate instantly with your current setup, remove manual tasks, and let ISMS.online do the hard work for you.

- **Seamlessly integrate with the way you work today**
- **Leverage the power of integrations in minutes**
- **Connections available with over 5,000 platforms**

“WE’VE MADE MORE ISO 27001 PROGRESS IN THE LAST TWO WEEKS USING ISMS.ONLINE THAN WE HAVE IN THE PAST YEAR.

TOM WOOLRYCH,
SERVICE & SUPPORT MANAGER
THE WORKFORCE DEVELOPMENT TRUST



isms.online

See how ISMS.online can help your business

Book a tailored, hands-on session based on your needs and goals

Book your free demo →