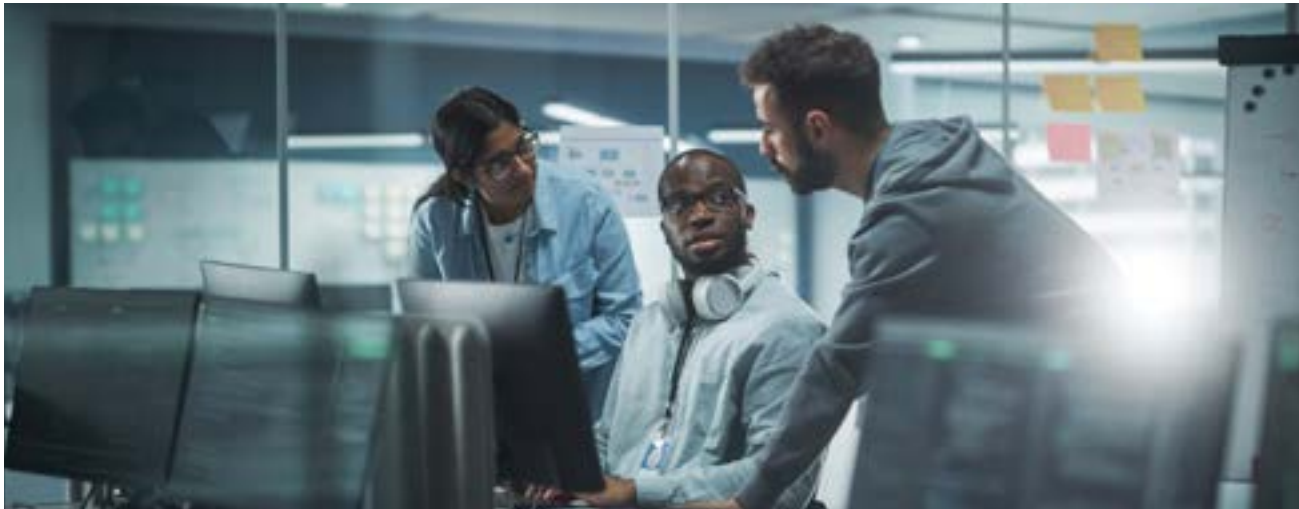


NIS2 Directive: Stricter requirements for cyber security

The NIS2 directive is an EU-wide legislation that aims to increase the level of cybersecurity within the European Union. It does so, among other things, by addressing a wider range of industries, mandating stricter cybersecurity measures to be implemented (incl. cybersecurity risks in the supply chains) and creating stricter incident reporting requirements.

European Union (EU) member states have until September 2024 to translate the NIS2 directive into national implementing acts. These will be binding by law, meaning your organisation (if within scope) will have to comply with the requirements.


















Organisations in scope

The NIS2 directive is intended for medium or large organizations, and now provides an extended list of sectors that are subject to the regulation.

Organisations are classified (based on size and sector) as “essential entities” or “important entities”. The classification influences the responsibilities that organizations have when NIS2 comes into effect.

Note: the NIS2 directive lists exceptions on the size-cap rule and sector classification. See [Chapter 1 - Article 2 & 3](#)

Sector	Sub sector	Large sized 250+ employees or 50+ million revenue	Medium sized 50-250 employees or 10-50 million revenue
 Energy	electricity, gas, oil, heating/cooling, hydrogen, EV charging point operators	Essential	Important*
 Transport	air, rail, road, and water (incl. shipping companies and port facilities)	Essential	Important*
 Banking & finance	credit institutions, financial market infrastructure, trading venues, central counterparties (attention: DORA)	Essential	Important*
 Health	healthcare providers, research laboratories, pharmaceuticals, medical device manufacturing	Essential	Important*
 Water	drinking water suppliers, wastewater operators (only if it is an essential part of their general activity)	Essential	Important*
 Digital infra & IT services	trust services, DNS, TLD name registries, public electronic communications networks	Essential	Essential
	internet exchange, data centres, cloud computing, managed (security) services	Essential	Important*
 Public administration	central government (excl. judiciary, parliament, central bank; defence, national / public security)	Essential	Essential
	regional government: risk based, local government: optional	Important*	Important*
 Space	operators of ground-based infrastructure	Essential	Important*
 Postal and courier services		Important*	Important*
 Waste management	(only if principal economic activity)	Important*	Important*
 Chemical products	manufacture, production, distribution	Important*	Important*
 Food	production, processing, distribution	Important*	Important*
 Manufacturers	medical devices; computers, electronics, optics, machinery, motor vehicles, trailers, other transport equipment	Important*	Important*
 Digital providers	online marketplaces, search engines, social platforms	Important*	Important*
 Research organisations	(excluding education institutions)	Important*	Important*

* Important, except if identified as Essential by Member State

Cybersecurity risk-management requirements

When implemented, NIS2 will increase the (minimal) effort that organizations should spend on cybersecurity. In Summary, the NIS2 directive sets requirements for:

Risk Ownership

Management are given direct responsibility for ensuring that cyber risks are identified, addressed and requirements are met. [Chapter IV - Article 20](#)

Risk Control

Your organization must implement both prevention and mitigation measures that reduce risks and impacts. Such as, adequate measures around incident management, cyber security in supply chains, network security, access control and encryption.

Business Continuity

Your organization should consider how to ensure business continuity if you are hit by a major cyber incident. For example, system recovery, emergency procedures and setting up a crisis organization.

Incident Reporting

Organisations must ensure proper reporting to authorities. Among other things, there is a hard requirement that major incidents are reported within 24 hours and an initial assessment is performed within 72 hours. [Chapter IV - Article 23](#)

More specifically, Article 21 in the NIS2 directive explicitly listed the following technical, operational and organisational measures to manage the risks posed to the security of network and information systems, and to prevent or minimise the impact of incidents: [Chapter IV - Article 21](#)

- a. policies on risk analysis and information system security;
- b. incident handling;
- c. business continuity, such as backup management and disaster recovery, and crisis management;
- d. supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- e. security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure;
- f. policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- g. basic cyber hygiene practices and cybersecurity training;
- h. policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- i. human resources security, access control policies and asset management;
- j. the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

Supervision and enforcement

Organizations that are classified as Essential entities can expect to be subject to on-site and off-site supervision, including random checks. And annual and targeted audits, based on risk assessment outcomes or risk-related available information.

Under NIS2, authorities have the power to hold management personally accountable if gross negligence is proven after a cyber incident. For Essential entities, it empowers authorities to temporarily stop a person from exercising managerial positions in case of repeated negligence.

[Chapter VII - Article 32](#)

Organizations that are classified as Important entities will be subject to reactive supervision by authorities as opposed to proactive supervision reserved for Essential entities. This means that unless there is a reason for it, such as a cyber incident or reports from external organisations such as auditors or other parties in the supply chain, an Important entity will not face direct supervision from regulators and authorities.

[Chapter VII - Article 33](#)

The sanctions are extended by the NIS2 directive to include fines based on global turnover. These penalties are based on whether organizations are part of an Essential entity or an Important entity. For Essential entities, they are based on a minimum of ten million euros, or 2% of global annual turnover, whichever is higher.

For Important entities, fines are based on a minimum of seven million euros or 1.4% of turnover.

[Chapter VII - Article 34](#)



About Ivanti

Ivanti elevates and secures Everywhere Work so that people and organizations can thrive. We make technology work for people, not the other way around. Today's employees use a wide range of corporate and personal devices to access IT applications and data over multiple networks to stay productive, wherever and however they work. Ivanti is the only technology company that finds, manages and protects every IT asset and endpoint in an organization. Over 40,000 customers, including 88 of the Fortune 100, have chosen Ivanti to help them deliver an excellent digital employee experience and improve IT and security team productivity and efficiency. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit [ivanti.com](https://www.ivanti.com)

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".A vertical bar on the right side of the page, transitioning from red at the top to orange at the bottom.

[ivanti.com](https://www.ivanti.com)

1 800 982 2130

sales@ivanti.com