Columbus®

# Breaking down the upcoming EU NIS2 legislation

Get Started

What is NIS2?

The NIS 2 directive is a set of proposed EU legislation that builds upon existing rules around Cybersecurity. It aims to address current weaknesses in organizations' Cyber security obligations in a world where the pandemic and geo-political instability have highlighted threats to energy and food supply chains. With streamlined reporting obligations, increased supervisory measures and stricter enforcement requirements, the legislation aims to boost the level of cybersecurity in Europe long term.

Which Countries are affected?

All EU member states will be expected to implement the legislation. By association, non-member states such as Norway and the UK will need to be compliant due to strong trading links with nations within the union.
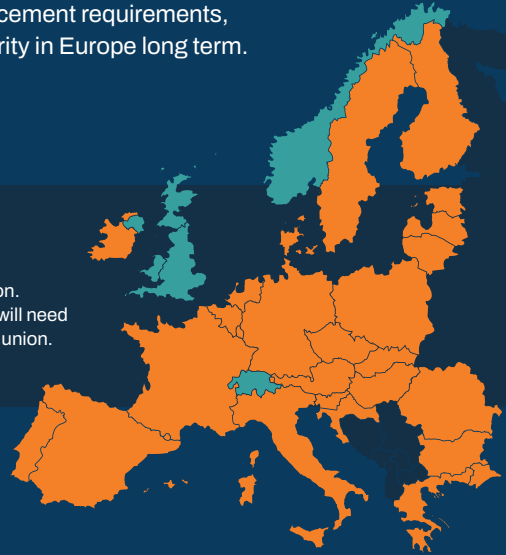
Which industries are affected?

The scope of NIS2 Directive covers industry sectors representing the highest societal risks and are broken down into two groups:

Very small companies of 49 employees or less are not affected by NIS2.

Critical Sectors

- **Energy -** electricity, oil, gas, heat, hydrogen
- **Health -** providers, labs, R&D, pharma
- **Transport -** air, rail, water, road
- **Banks and financial markets**
- **Water and wastewater**
- **Digital -** IXP, DNS, TLD, DC, CSP, CDN, TSP
- **Space**
- **Public Administration**

Important Sectors

- **Postal and courier**
- **Waste management**
- **Chemicals**
- **Food**
- **Industry -** technology and engineering
- **Digital services -** social, search, markets

Why NIS2 and how can organizations benefit?

Increased industry collaboration and reporting will mean that bodies working together along supply chains will share information rapidly. You will know more, faster and be able to coordinate a better response to protect the continuity of not only your business, but customers and partners alike.

NIS2 puts focus on embedded risk management within affected entities, all organizations within your sector will have to prove adoption of a policy and procedure to identify and assess Cyber risks regularly. A rising tide lifts all boats and once again, better coordination of the management of risk up and down key value streams and supply chains will lead to a more resilient and better-protected global economy.

Focus on the people-related aspects of Cybersecurity will translate into a better-informed workforce who are granted access to just the right information only when it is needed. The just-in-time approach to access control in applications such as ERP can prevent key intellectual property enshrined in data such as bills of material or production routings being shared with unauthorized persons leading to the loss of competitive advantage.

What is expected of organizational leadership and management?

If you are within an affected state and industry sector, your management will be expected to be responsible and accountable for:

The approval of cybersecurity risk management measures at C-Level

Supervision of the implementation of the risk management measures operationally

Ensuring that specific, regular training and awareness is carried out to gain Cyber-defence capability and to assess associated risks to their organization

Any non-compliance of the organization.

What are the key elements to be addressed within your business?

Cybersecurity measures – applicable to all entities

What? How can Columbus help?

Risk Analysis

Technical assessment of key services and infrastructure in the Cloud or on-premise.

Analysis of critical business processes and advisory on relevant mitigations.

Security in Networks and Information systems Acquisition

Columbus is an ISO 27001 compliant business with robust implementation and development processes.

Choosing us as your Digital Transformation partner ensures secure acquisition of services.

Incident Handling

Evidence gathering through technical forensics working alongside your team to manage incidents in a timely manner.

Sourcing and coordination of response as a key supplier working with your IS team and other key partners such as Microsoft.

Testing and Auditing

Assistance with business continuity testing Security Audit support, by provision of log analytics and intelligent alerting to risks to key data and configuration in applications.

Monitoring of key security events and notification to assist in meeting NIS2 reporting deadlines.

Business Continuity

Advisory, architecture and implementation of processes and procedures to achieve recovery time objectives.

Policy on Cryptography and Encryption

Advisory on how Cryptography is applied to protect key information within your SaaS applications and the services they integrate with in the Microsoft cloud and beyond.

Supply Chain Security

Industry knowledge of critical links within your supply chain and advisory on measures to lessen the impact of any future breach, through digital, data driven means.

Human Resources Security

Columbus provide a best-in-class access management services which ensures that segregation of duties and least-privilege access is applied to the data within your key cloud applications such as Dynamics 365 ERP.

Standards

Affected organizations may be mandated to use certain products, processes, or services under specific EU certification schemes. It is not yet known which these will be, but companies can prepare by ensuring that they have attained a relevant information security quality standard, such as ISO27001 which covers many of the requirements impacted by NIS2.

Reporting and information sharing

Entities operating under NIS2 will be required to notify incidents to the member states "competent authorities" within 24 hours of becoming aware of them and ensure that information exchange takes place between appropriate organizations within trusted communities. A full report would be expected within 1 month of the initial notification.

Registration

Member states will have a duty to disclose the entities in scope of NIS2 to a central register managed by ENISA, the EUs central Cyber Security agency. Other member states may be granted access to the information held in this registry as part of co-ordinated cross-border incident response.

What is the impact of non-compliance?

Organizations found the be in violation of the legislation may face fines of up to 10 million euros or 2% of annual global turnover. Of course, the reputational impact of any incident resulting in non-compliance when made public would be incalculable.

What is the adoption timeline?

A proposed text was agreed upon in May 2022. It is expected that NIS 2 will be adopted in late 2022 and the requirement to transpose it into national laws will need to be carried out within 18-21 months afterwards. Organizations need to act now to ensure readiness in accordance with this timeline.

Where can I find out more about the impact on my Cloud ERP and other applications?

More details on NIS2 and its impact can be found by following the link below:

More details

The NIS2 Directive: A high common level of cybersecurity in the EU | Think Tank | European Parliament (europa.eu)

If you'd like to explore how Columbus can support you in becoming compliant in the way you operate your SaaS applications, such as Dynamics 365, Power Platform and the broader set of Microsoft Azure services, reach out to us today.

Contact us today

About Columbus:

Columbus is a global IT services and consulting corporation with more than 2,000 employees serving our customers worldwide. We bring digital transformation into your business and position you to thrive far into the future. We are experts in designing, developing, implementing, upgrading and maintaining digital business applications that help your business succeed in the digital transformation. Our consultants have experience in developing businesses in many different industries all over the world. We offer a comprehensive solution portfolio with deep industry knowledge, extensive technology expertise and profound customer insight. We have proven this through 30 years of experience serving more than 5,000 customers worldwide.

Application Management | Ensure stable business applications and digital platforms that evolve with business needs columbusglobal.com