New Cybersecurity regulatory requirements

NIS2: Network and Information Security Directive 2

NIS2 expands the scope of the older NIS1 regulation, by adding 11 new sectors, requiring a plethora of new organisations to follow the cybersecurity regulation.

It is estimated that about 700 organisations are going to be affected in Cyprus alone and over 150,000 across the EU.

Affected organisations will be required to review, test and upgrade their security controls, as well as catch up with new incident reporting obligations.

» Background

The NIS2 Directive sets up requirements for the EU member states' cyber and information security. It requires that member states must develop and adopt national cyber and information security strategies and designate a national point of contact for cybersecurity incidents.

» Timeline

NIS2 came into effect

1. **Oct 2024**
   Adopt and publish measures
2. **Jan 2025**
   Progress assessment
3. **Apr 2025**
   List "Essential" and "Important" entities
4. **Oct 2027**
   Directive revision

» Affected Industries

Highly Critical - Covered by NIS1

- Energy
- Transport
- Banking
- Financial Market Infrastructures
- Health
- Drinking Water
- Digital Infrastructure

- Water waste
- ICT Service Management
- Public Administration
- Space

Expanded by NIS2

Other Critical

- Waste Management
- Postal/Courier Services
- Research
- Manufacturing
- Digital Providers
- Production & Distribution of Chemicals
- Production & Distribution of Food

» Main requirements

- Policies on risk analysis and information system security
- Incident handling
- Business continuity
- Supply chain security
- Security in network and information systems acquisition, development and maintenance
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- Implement up-to-date cryptography/encryption and network controls
- Basic cyber hygiene practices and cybersecurity training
- Human resources security, access control policies and asset management
- Use multifactor authentication and other secure authentication solutions.

» Overview of PwC Services

Scoping

Determine compliance needs. Identify critical processes and assets in scope and identify critical assets' dependencies.

Cybersecurity capability maturity assessment

Assess the existing level of cybersecurity maturity. Identify areas of potential improvements to be compliant with both ISO27001 and NIS2.

Impact assessment

Assessment of threats and risks. Assess the current risk landscape to identify critical areas of vulnerability. This involves an examination of potential threats and the impact they could have on your operations.

Readiness assessment

Identify organisational, legal and technical gaps against the requirements and current maturity levels.

» Contacts

Sophie Solomonidou
Director
Risk Assurance Services
+357 99609585
sophie.solomonidou@pwc.com

Michael Solon Kassini
Manager
Risk Assurance Services - Digital Trust
+357 96555143
michael.s.kassini@pwc.com