Solution Brief

Insight NIS2 Assessment Service

Are you ready for the new directive for Network Information Security (NIS2)?

Background

The new directive NIS2 will come into force on 18th October 2024, designed to improve the resilience and security of the network and information systems within the EU. It has expanded the breadth and depth of the original directive with more comprehensive security controls, rigorous incident reporting requirements and increased enforcement measures with sanctions.

The list of sectors in scope has increased and there is a distinction made between essential and important companies.

The sectors NIS2 will apply to

Essential Sectors	Important Sectors
Energy	Postal Courier Services
Transport	Waste Management
Banking	Chemicals
Financial Market Infrastructure	Food
Health sector	Manufacturing of Medical Devices
Drinking water	Digital Providers
Wastewater	Research Organisations
Digital Infrastructure	
IT Service Management	
Public Administration	
Space	

Essential Sectors
Large companies with 250 or more employees, 50 million euros in annual revenues and/or total balance assets of 43 million euros or more.

Essential/Important Sectors
Medium-sized companies with 50 or more employees, 10 million euros in annual revenues and/or total balance assets of 43 million euros or more.

How Insight can help

Insight can help you prepare and be ready to comply with the new NIS2 directive by assessing your current state and identifying any gaps and improvements that need to be addressed to achieve compliance.

Areas to focus on

- Risk analysis
- Business continuity
- Supply chain security
- Security of network information systems
- Incident handling
- Effectiveness
- Human factors
- Cryptography and encryption
- Physical security
- Multi-factor authentication

Our solution

Insight's security and compliance experts will provide an assessment based on the European NIS2 guidelines.

The National Cyber Security Centre (NCSC) has published 14 high-level security principles that must be implemented in the form of the Cyber Assessment Framework (CAF).

Managing security risk	▪ Governance ▪ Risk management ▪ Asset management ▪ Supply chain
Protecting against cyber attack	▪ Service protection policies and procedures ▪ Identity and access control ▪ Data security ▪ System security ▪ Resilient networks and systems ▪ Staff awareness and training
Detecting cyber security events	▪ Security monitoring ▪ Anomaly detection
Minimising the impact of cyber security incidents	▪ Response and recovery planning ▪ Improvements

Our assessment will include the following elements

- **Kick-off call:** establish goals and plan of activities
- **Assessment:** documentation analysis and series of interviews
- **Workshop:** to discuss findings and possible areas of improvements
- **NIS2 assessment documentation:** Detailed report and next steps.

Insight can then provide additional services to support you to remediate and meet your obligations and improve your security to achieve NIS2 compliance.

Visit our uk.insight.com and connect with your Insight account representative to get additional resources and assistance.

About Insight

At Insight, we have the expertise, skills, tools, processes, and experience to guide you towards achieving your full potential and optimising the competitive advantage.

Global scale & coverage	Operational excellence & systems	Next-generation tech skills	A certified and award-winning partner of major security solution vendors	Understanding of ISO 270001	Broad security capabilities

For more information please contact your Insight Account Manager.

+32 (0)2 263 60 20 | contactus@insight.com | be.insight.com