NIS2

Strengthen your organisation and stay secure with NIS2

With the rise of digital threats and the growing number of cyberattacks, the risk of disruption to critical business processes has significantly increased. The new European Directive on digital resilience (NIS2) is a legal requirement that imposes stricter standards for the security of network and information systems. It is expected that larger organisations will need to implement the NIS2 Directive by the third quarter of 2025. By acting now, you will strengthen your organisation's security and future-proof its operations.

What does the NIS2 Directive mean for your organisation?

The NIS2 Directive applies to larger organisations in sectors such as healthcare, energy, transport, banking and digital infrastructure, including suppliers.

If your organisation falls into one of these sectors, you have a legal obligation to take appropriate measures to strengthen your cybersecurity and to report incidents promptly. Failure to comply can result in significant fines, reputational damage and loss of customer confidence. At the same time, NIS2 presents an opportunity to make your organisation more secure and resilient against future threats.

* Small businesses (fewer than 50 employees and turnover under €10 million) are exempt from the NIS2 Directive.

What are your responsibilities under the NIS2 Directive?

Duty of care: You are required to take appropriate technical, organisational and process controls to minimise risks to your network and information security. This includes establishing a comprehensive risk management framework and incident response protocol.

Duty to report: Major security incidents must be reported within 24 hours, followed by a detailed report within 72 hours. Immediate action is essential to comply with the requirements of NIS2.

Contact us

Ensure your organisation is NIS2-compliant. Act now for a tailored security assessment and action plan. **Get in touch** to strengthen your digital resilience.

Our approach to helping you comply with the NIS2 Directive

1. **Baseline assessment:** We start with a detailed assessment of your existing security posture to determine where your organisation's cybersecurity posture.
2. **Gap analysis:** We identify gaps against NIS2 requirements and develop a prioritised action plan.
3. **Implementation:** We assist you in implementing both technical and organisational security measures to meet NIS2 standards.
4. **Validation testing:** After implementation, we assess the effectiveness of the measures and ensure you are prepared for audits and inspections.

Why Sopra Steria?

Sopra Steria, a major technology player in Europe with 52,000 employees in nearly 30 countries, is recognised for its consulting, digital services and solutions. It helps its clients drive their digital transformation and achieve tangible and sustainable benefits. The Group provides end-to-end solutions to make large companies and organisations more competitive by combining in-depth knowledge of a wide range of business sectors and innovative technologies with a collaborative approach. Sopra Steria puts people at the heart of everything it does and is committed to making digital work for its clients to build a positive future for all. In 2023, the Group will have revenues of €5.8 billion.