The Network and Information Systems Directive (NIS)

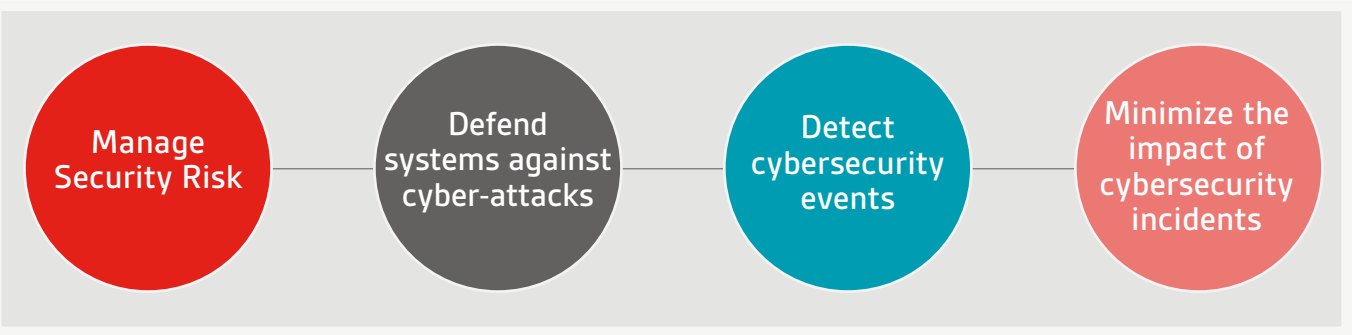
bsi.

...making excellence a habit.™

The Network and Information Systems (NIS) Directive is an EU wide piece of legislation aimed at increasing the level of cybersecurity for critical infrastructure including utilities, transport, healthcare and digital services and to give them the opportunity to deploy best practice cybersecurity protocols.

This framework nurtures sustainability, mitigates risks, protects organizations and their information, safeguards their people and ensures a state of enhanced information resilience.

NIS Directive main objectives are to help organizations:



The NIS Directive sets out 14 Principles by which to define, measure and improve cybersecurity.

With the ever-increasing growth of cyber-attacks, employing the tenets of the NIS Directive is imperative. A prevention-only based cybersecurity strategy is not enough, organizations must plan for resilience through rapid detection and practiced response.

NIS Directive compliance became a legal requirement for Operators of Essential Services (OES) in 2018. Each OES will have a corresponding competent authority depending on their sector, for example OFGEM is the CA for OES in the Gas and Electricity sectors.

The role of the competent authority is to ensure that the OES complies with the NIS Directive requirements and they may take enforcement action if deemed appropriate.

It is a slightly different approach for Digital Service Providers (DSP) who are deemed critical to the ongoing good running of a country, in that they must themselves assess whether they are in scope or not for the NIS Directive, allowing for some ambiguity in this space.

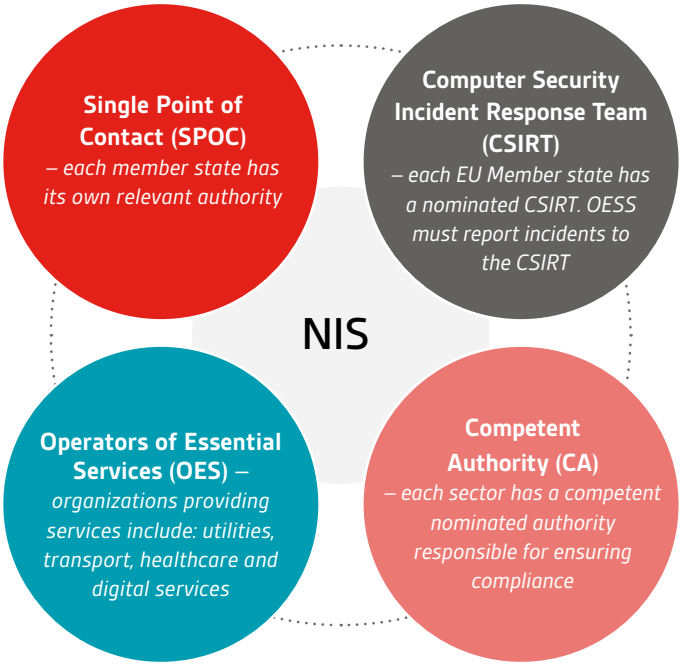
Achieving NIS compliance

The UK National Cyber Security Centre (NCSC) plays a key role in setting the approach for embedding the NIS Directive in the UK's critical infrastructure. The NCSC has deliberately steered away from defining a prescriptive set of security controls by which to achieve NIS compliance and an implied sense that effective cybersecurity is achieved.

The approach taken by the NCSC is to define a set of principles which the organization must interpret and apply within their own context and circumstances.

Managing security risk is key to meeting the requirements of the NIS Directive. This is a complex task, but the right advice and expert support will make the journey to achieving proportionate and effective security controls quicker and more cost effective.

NIS entities



The NIS journey

Familiarize with the legislation | Connect with competent authority | Understand reporting requirements | Carry out self-assessment | Risk management | Risk treatment

Familiarize with Legislation

If your organization is involved with the provision of essential services in the energy, transport, healthcare, drinking water or digital infrastructure sectors you may be classified an OES. The NIS legislation has detailed guidance for OES, available here: https://www.legislation.gov.uk/uksi/2018/506/made

BSI can help interpret the legislation so you can understand if the regulations apply to you.

Connect with Competent Authority

Operators of Essential services should work with their competent authorities. Competent authorities have NIS information on their websites including contact information for OES and points of contact for incident reporting. Most competent authorities have published guidance for OES in their sectors.

Understand Reporting Requirements

Competent authorities require OES to provide them with a report on how they meet the NIS Directive requirements, identifying any gaps in their compliance with the requirements and demonstrating how related cybersecurity risks are managed. Most CAs provide a template to support reporting. In the UK the templates are based on the National Cyber Security Centre's Cyber Assessment Framework or CAF.

Carry out Self-Assessment

The Cyber Assessment Framework (CAF) offers a self-assessment tool based on the 14 principles of the NIS Directive. Each principle has a corresponding set of indicators of good practice that can be used to assess compliance. BSI's team of experienced cybersecurity consultants can support OES in their self-assessment process from defining the scope to assessing the controls.

Risk Management

The assessment process is likely to identify some control gaps and it is important that the risks associated with the control gaps can be articulated, prioritised and managed. This is a critical factor for CAs to gain confidence in the OES ability to deploy proportionate levels of security controls and to make mature risk-based decisions.

Risk Treatment

Risk treatment should be prioritised based on the criticality of the risk identified. Because the scope of the NIS Directive is broad, risk treatment could take the form of anything from policy and process development to security awareness training or deployment of technical security controls including re-design of existing systems.

Many of the OES who operate OT or SCADA industrial control systems may not have upgrade paths available short of complete system replacement and in some instances, bringing forward system replacements may need to be considered.

The table below reflects the level of difficulty that clients face in addressing self-assessment findings under the different principles.

This is based on BSI consultants' experience when working on similar engagements with clients.

Ref	NIS principle	Difficulty to address
A1	Governance	Low
A2	Risk Management	Medium
A3	Asset Management	High
A4	Supply Chain	Medium
B1	Service protection policies and processes	Medium
B2	Identity and access control	Medium
B3	Data security	Medium
B4	System security	High
B5	Resilient network and systems	Medium
B6	Staff awareness training	Medium
C1	Security monitoring	High
C2	Proactive security event discovery	Medium
D1	Response and recovery planning	Medium
D2	Lessons learned	Medium

How can BSI help?

From initial OES identification to self-assessment, risk assessment and risk treatment, our experience of working with organizations across the sectors can help you to navigate the pathway to NIS Directive compliance.

Achieving NIS compliance

Provide access to consultants with vast industry experience and in-depth cybersecurity expertise.

Engage with stakeholders across the business to interpret the principles and make them relevant.

Deliverable: Scoping workshop with an expert BSI consultant.

Evaluate how the organization currently meets the requirements and identify any gaps or areas where improvements are necessary.

Deliverable: Detailed assessment of current organization activities.

Prioritize and target any necessary remediation activity to ensure maximum security improvement and return on investment.

Deliverable: Roadmap to compliance.

Support ongoing communication with internal and external stakeholders.

Deliverable: Opportunity to leverage a comprehensive set of products, services and experienced consultants.

In addition to the services outlined above, the table below further describes the services BSI provides which addresses the 14 principles of NIS Directive.

Cybersecurity services	Cloud security solutions	Vulnerability management	Incident management	Penetration testing/red teaming	Virtual CISO	TP security/ risk assessment
Information management and privacy	eDiscovery eDisclosure	Digital forensics	Legal tech	Data protection services	Data subject requests	DPO as a service
Security Awareness and Training	End user awareness	Phishing simulations	Social engineering	Certified Info tech training	Onsite and bespoke training	Online interactive solutions
Compliance services	PCI DSS	NIST	ISO/IEC 27001 management	Accredited cyber-lab	Data protection	GDPR
NIS principle						
A1 Governance	● ● ●	● ●	● ●	●	● ● ● ●	●
A2 Risk Management	●	●	●	●	●	●
A3 Asset Management	●	●	● ●	●	●	●
A4 Supply Chain	●	●	● ●	●	●	●
B1 Service protection policies and processes	●	●	●	●	●	●
B2 Identity and access control	●	●	●	●	●	●
B3 Data security	●	●	●	●	●	●
B4 System security	●	●		●	●	●
B5 Resilient network and systems	●	●	●	● ●	●	●
B6 Staff awareness training	●	●	●	● ●	●	●
C1 Security monitoring	●	●	●	●	●	●
C2 Proactive security event discovery	●	●	● ●	●	●	●
D1 Response and recovery planning	●	●	● ●	●	●	●
D2 Lessons learned	● ● ● ●	● ● ● ●	● ● ● ●	● ● ● ●	● ● ● ●	● ● ● ●

The NIS Regulations post-Brexit
The UK Government has confirmed that the NIS Regulations will continue to apply in the UK after Brexit.

Impact for Business: DSPs established in the UK (and not established in the EU), which offer services within the EU, should establish plans to appoint a representative in the EU post-Brexit. Similarly, DSPs established outside of the UK, which offer services within the UK, should establish plans to appoint a representative within the UK post-Brexit.

DSPs that will be subject to both the NIS Regulations and Member State domestic law giving effect to the NIS Directive should consider implementing procedures to ensure regular monitoring and effective and efficient compliance with each regime. Failure to comply with the relevant requirements of the NIS Regulations in the UK exposes organizations to enforcement action, including the imposition of fines of up to £17 million.

bsi.

Find out more:

UK
Call: +44 345 222 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com/cyber-uk

IE/International
Call: +353 1 210 1711
Email: cyber.ie@bsigroup.com
Visit: bsigroup.com/cyber-ie