OES Operators of Essential Services

The NIS Regulations

The UK's Network and Information Systems Regulations 2018 (NIS Regulations) are derived from the EU's Directive on security of network and information systems (NIS Directive), and aim to achieve a high, common level of network and information systems security.

Objectives

To improve national cyber security capabilities.

For OES to take "appropriate and proportionate" security measures, and notify relevant competent authorities of serious incidents.

To increase co-operation between EU member states.

What is an OES?

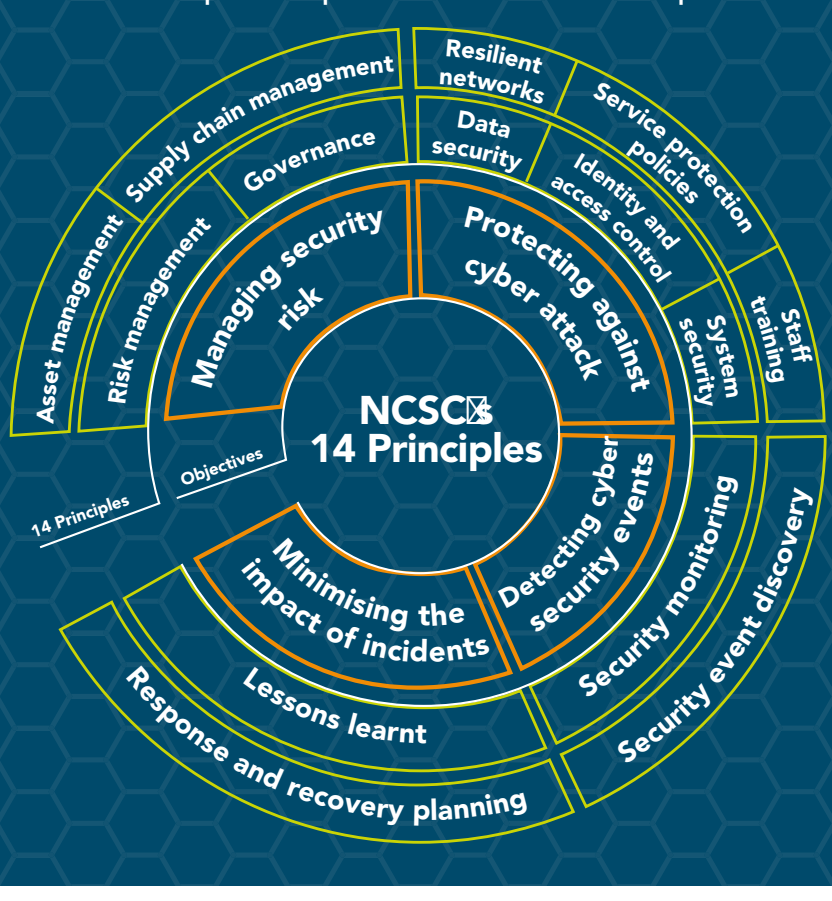
There are critical business sectors that, if services were disrupted, would have a profound impact on the society or the economy. The NIS Regulations aims to bolster cyber security to improve the network and information security across these sectors.

The NIS Regulations list the following sectors of OES:

- Energy
- Transport
- Digital infrastructure
- Healthcare
- Water

Compliance requirements

The NCSC has published **4 top-level objectives**, which are broken down into **14 high-level principles**. OES are expected to implement these principles in their compliance project.



Cyber Assessment Framework (CAF)

OES will be subject to regular audits by competent authorities.

The CAF has been developed around the **14 principles** and each principle has IGP (indicators of good practice).

The CAF will be used as an auditing framework by competent authorities for judging compliance.

Compliance levels against the IGPs:

Competent authorities

In the UK, competent authorities are appointed for each sector and provide compliance guidance to organisations, as well as enforcing the requirements of the law.

The NIS Regulations came into force on

10 May 2018

The role of competent authorities

Competent authorities have been identified for each sector. A full list can be found in the NIS Regulations.

- Monitor the application of the NIS Regulations
- Direct OES to undertake actions in relation to NIS Regulations
- Request information related to the NIS Regulations
- Audit, or require an audit, of OES
- Designate OES
- Issue penalties to OES
- Prepare and publish guidance
- Investigate the causes of an incident
- Enforce an instruction on OES
- Notify the public about an incident

Incident Reporting

OES must report any incidents that occur to their competent authority within **72 hours** of becoming aware of the incident.

The incident reporting structure has been broken down into two sections:

Incident notification reporting structure

A notification phase, where an incident is reported by the OES and the competent authority decide if a follow-up is needed.

Incident response reporting structure

A response phase, where the NCSC, the competent authority, or lead government department should be approached for assistance by the OES.

Penalties for non-compliance

Intended to motivate enhancements to cyber resilience while being proportionate to potential risks.

Competent authorities will define the fines **by sector.**

A maximum fine of up to **£17 million** can been levied in the UK.