0345 340 5412
info@dataprotectionpeople.com

NIS Regulations: Cyber Assessment Framework

The EU Directive on the security of Network and Information Systems (NIS) was introduced to improve the security of critical infrastructure and essential services. The UK Government has decided, as with GDPR, that 'Brexit' will not affect its implementation. The NIS Directive was brought into UK law on 10 May 2018, with the The Network and Information Systems Regulations 2018.

All organisations that are considered to be 'Operators of Essential Services' are legally required to comply with the Regulations. Essential Services include: electricity; oil; gas; air, maritime, rail , and road transport; water; healthcare; and, digital infrastructure.

Fines for non-compliance can be as high as £17 million, in addition to those already provided for by the GDPR. In support of the Regulations, the National Cyber Security Centre has developed the Cyber Assessment Framework, which regulators will use to assess your organisation's cyber security.

Why choose us?

We have a detailed working knowledge of both critical national infrastructure issues, and the NIS Regulations. Our team has conducted threat assessments and capability audits, for aerospace, shipping, and defence (including on the ground in Afghanistan).

They hold industry qualifications such as CESG Certified Professional (Information Assurance Audit), Certified Information Systems Auditor, BSI Lead Auditor, and Certified Information Systems Security Professional.

How we can help you

Scope Assessment

Identifying the scope of your critical systems is a vital part of compliance with the NIS Regulations. Our consultants will help you to correctly identify which systems impact on your provision of essential services, and how these systems are affected by the issues identified by your Threat Model.

Gap analysis

Our CESG Certified consultants will conduct an on-site assessment to identify key areas of weakness within your physical, digital, and process infrastructure. They will inspect your security controls, in line with the requirements of the Cyber Assessment Framework. At the end of the Gap Analysis, you will receive a report detailing your current strengths and weaknesses, complete with actionable points. This report will provide you with the information you need to fix any identified weaknesses.

Remediation

We can work with you to fix any issues identified by the Gap Analysis–a process known as remediation. This remediation work puts your organisation in a position to achieve compliance with the NIS Directive. We can help you to implement process, procedure, and technical controls.

Mock audits and external inspection support

The Network and Information Systems Regulations provide your sector's Competent Authority with a power of inspection. Our consultancy team can attend your site during an inspection, to support your team, and liaise directly with the inspectors.

We are also able to conduct a mock inspection, led by our CESG Certified Information Assurance Auditors, providing you with assurance of your systems. A mock inspection is a fantastic way to pre-empt any issue that could occur during an external inspection by your sector's Competent Authority.