The EU Directive on Security of Network and Information Systems (NIS Regulations)

UK compliance guidance

April 2018

The NIS Directive

UK compliance guidance

Introduction

First proposed in 2013 as a means of implementing the Juncker Commission's EU Cybersecurity Strategy,[1] the NIS Directive **(Directive (EU) 2016/1148)** aims to achieve a high common level of network and information systems security across the European Union by:

- Improving national cyber security capabilities;
- Increasing cooperation between EU member states; and
- Requiring "operators of essential services and digital service providers" to take appropriate and proportionate security measures, and notify the relevant national authorities of serious incidents.

The Directive was adopted by the European Parliament on 6 July 2016, and entered into force on 8 August 2016.

EU member states have until 9 May 2018 to translate the Directive into national laws – which must apply from 10 May 2018 – and a further six months to identify **operators of essential services (OES)**.

The UK government's Department for Digital, Culture, Media and Sport (DCMS) consulted with relevant industry bodies and organisations in developing its approach to the Directive. The government has now responded to the consultation,[2] the outcomes of which are clarified in this green paper.

A note on Brexit

The UK is due to formally leave the EU on 29 March 2019, just under a year after the Directive applies. It is the government's intention that the Directive will continue to apply after the UK leaves the EU.

As the government's response to the consultation states:

> Until exit negotiations are concluded, the UK remains a full member of the European Union and all the rights and obligations of EU membership remain in force. During this period the Government will continue to negotiate, implement and apply EU legislation. The outcome of these negotiations will determine what arrangements apply in relation to EU legislation in future once the UK has left the EU. It is the UK Government's intention that on exit from the European Union these policy provisions will continue to apply in the UK.

Applicability

Annexes II and III of the NIS Directive set out the types of OES and **digital service providers (DSPs)** that its requirements will apply to. Micro and small enterprises do not fall under the scope of the Directive, however.[3]

Operators of essential services

OES are public or private entities that provide "a service which is essential for the maintenance of critical societal and/or economic activities; the provision of that service depends on network and

information systems; and an incident would have significant disruptive effects on the provision of that service".

The Directive deems the following sectors essential:

- **Energy** (electricity, oil and gas)
- **Transport** (air, rail, water and road)
- **Banking** (credit institutions)*
- **Financial market infrastructures** (trading venues and central counterparties)*
- **Health** (healthcare providers)
- **Water** (drinking water suppliers and distributors)
- **Digital infrastructure** (Internet exchange point (IXP) operators, domain name systems (DNS) service providers and top-level domain (TLD) name registries)

There is a comprehensive table of criteria (reproduced in the **Appendix** to this paper) to help identify OES in five of the seven sectors listed above.

* In line with Recital 9 of the Directive, OES in the **banking and financial market infrastructures** sectors are not in the Directive's scope, as they are already covered by equivalent provisions set by the Bank of England and the Financial Conduct Authority.

In addition to the organisations included above, some operators in certain sectors can be considered to provide an essential service even though they do not meet the proposed criteria.

The UK government is proposing a reserve power to designate these organisations OES. It only intends to use this power where there are valid reasons on the grounds of national security, threats to public safety or where a disruptive incident has the potential for significant adverse social or economic impact.

Digital service providers

DSPs are "any legal person that provides a digital service":

- **Online search engines** (Defined by the government as "a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input and returns links in which information related to the requested content can be found".)
- **Online marketplaces** (Defined by the government as "a digital service that allows consumers and/or traders [as defined in Directive 2013/11/EU] to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace".)
- **Cloud computing services** (Defined by the government as "a digital service that enables access to a scalable and elastic pool of shareable computing resources", which it further states "primarily (but not exclusively)" includes:
    - 'Infrastructure as a Service' (IaaS). IaaS refers to the delivery of virtualised computing resource as a service across a network connection, specifically hardware – or computing infrastructure – delivered as a service.
    - 'Platform as a Service' (PaaS). PaaS provides developers with environments on which they can build applications that are delivered over the Internet, often through a web browser.

- ‘Software as a Service’ (SaaS), where the resources available to the customer through that software are changeable in an elastic and scalable way. The government considers that this will not apply to most online gaming, entertainment or VoIP services because the resources available to the user are not scalable, but it may include services such as email or online storage providers, where the resources are scalable.)

NB: Digital services do not include ordinary websites, which are not covered by the Directive.

DSPs outside the EU

The NIS Directive applies to DSPs that are headquartered outside of the EU but offer services within it. These must designate a representative in one of the member states in which they offer their services, and will fall under the jurisdiction of that member state.

Although it may be difficult to enforce the Directive on DSPs outside the EU, it is nonetheless an important point. After all, OES will essentially be limited to using the services of DSPs that comply with the Directive. In addition, common consumers and other organisations will also want the reassurance that the services they are using and investing in are reliable.

Penalties for non-compliance

The government has established a penalty regime for the NIS Directive[4]:

> [A] maximum financial penalty of £17 million, which will cover all contraventions

The government’s response to the consultation notes, however, that “the maximum penalty levels are precisely that, and should be reserved for the most severe cases, in an appropriate and proportionate manner”. This is in line with the government’s stated position on penalties under the EU General Data Protection Regulation (GDPR), which applies from 25 May 2018.

Improving national cyber security capabilities

The UK government will be pursuing “a multiple competent authority approach”, which means that a competent authority will be identified for sectors and industries as needed, with each given “adequate legislative powers to carry out their duties and adequate resources to carry out their functions”. Although it will not be a competent authority itself, the National Cyber Security Centre (NCSC) will remain “central to the successful implementation” of the NIS Directive.

The devolved administrations are being consulted separately on competent authority arrangements for Northern Ireland, Scotland and Wales.

The NCSC will be the UK’s computer security incident response team (CSIRT). The agency has four main responsibilities:

1. National cyber security management.
2. Supporting critical national infrastructure companies to handle cyber security incidents.
3. Promoting cyber security situational awareness across industry, academia and the public sector.
4. Providing the single international point of contact for coordination and collaboration between national computer emergency response teams (CERTs).

The NCSC will also operate as the technical authority for cyber security. This means that it will publish guidance and assessment tools to help competent authorities assess compliance with the regulations.

Risk management and incident reporting obligations for OES and DSPs

The Directive proposes that OES and DSPs adopt a "culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced" so that they do not face "a disproportionate financial and administrative burden".

Clarification of what this entails is provided in Recital 46: "Risk-management measures include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact. The security of network and information systems comprises the security of stored, transmitted and processed data."

Operators of essential services

Article 14 of the Directive states that OES must:

- "take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations". Those measures should "ensure a level of security of network and information systems appropriate to the risk posed";
- "take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services"; and
- "notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide".

The NCSC's guidance describes four objectives, each representing several sector-agnostic principles. These principles describe the "mandatory security outcomes to be achieved". The objectives and principles are supported by a Cyber Assessment Framework (CAF), which will provide a "systematic method for assessing the extent to which operators of essential services (OES) are achieving the outcomes specified by the 14 NIS principles". The CAF is due for release before the end of April 2018.

The competent authorities will determine "acceptable levels of cyber security […] through use of the CAF", as well as which incidents need to be reported once the Directive applies.

Importantly, the government "believes that there is no single existing standard that adequately covers NIS Directive requirements for operators of essential services".

In other words, they will need to ensure that whatever information security regime the organisation adopts meets the government's proposed security principles. (See **High-level security principles**, below.)

Digital service providers

Unlike OES, the Directive states that competent authorities should have "no general obligation to supervise digital service providers" and should "only take action when provided with evidence […] that a digital service provider is not complying with the requirements of this Directive, in particular following the occurrence of an incident" (Recital 60).

Recital 49 notes that "the degree of risk for operators of essential services […] is higher than for digital service providers. Therefore, the security requirements for digital service providers should be lighter. Digital service providers should remain free to take measures they consider appropriate to manage the risks posed to the security of their network and information systems".

Article 16 is more specific about the requirements for DSPs. They must:

- "take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services". These security measures should "ensure a level of security of network and information systems appropriate to the risk posed" and take account of:
  - The security of systems and facilities;
  - Incident handling;
  - Business continuity management;
  - Monitoring, auditing and testing; and
  - Compliance with international standards.
- "take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services [they offer], with a view to ensuring the continuity of those services".
- "notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service" that they offer.

Commission Implementing Regulation (EU)

The European Commission's Implementing Regulation[5] sets out the security measures and incident reporting thresholds for DSPs. This makes it clear that it is the DSP's responsibility to assess the scale of an incident, its geographical spread and the significance of damages to service users in the EU.

It also clarifies that the "appropriate and proportionate technical and organisational measures" noted above (Article 16.1) can be managed under the guidance of international standards.

Additionally, the Implementing Regulation defines the specific metrics for "substantial impact", which determine the DSP's duties in relation to notifying the competent authority. These metrics include:

- Service unavailable for more than 5 million user-hours in the Union.
- Loss of confidentiality, integrity, availability or authenticity of data accessed over networks or information systems that affects more than 100,000 users in the Union.
- Incident creates a risk to public safety, public security or loss of life.
- Material damage to at least one user in the Union exceeding €1 million.

The UK government carried out a consultation on the Implementing Regulation in March 2018, where it added occasional emphasis to certain recitals, but made no major amendments.[6] It also took the technical guidelines provided by ENISA[7] into account to "ensure that there is a consistent approach across Europe" for reporting incidents.

ENISA's guidance describes a system of security objectives that apply generally to DSPs, ranging from establishing an information security policy through to customer monitoring and log access. It also describes different levels of sophistication for each objective. This is reflected by a set of specific security measures of increasing sophistication, which can help an organisation pursue and attain greater maturity and improved compliance with the NIS Directive.

The Information Commissioner's Office (ICO) will be responsible for regulating DSPs.[8] While not required to explicitly identify DSPs, it will provide guidance to help them self-identify whether they are

within scope. The UK's targeted consultation on DSPs states that the ICO will "establish a system in order for UK DSPs to register themselves with the ICO" after 10 May 2018.[9]

The ICO will also clarify DSPs' security obligations and incident response requirements under the Directive, which will take ENISA's guidelines into account.

High-level security principles

The NCSC has defined four objectives for OES, each of which is divided into high-level security principles and supported by guidance from a range of sources.[10] These principles are:

1. Managing security risk.
2. Defending systems against cyber attack.
3. Detecting cyber security events.
4. Minimising the impact of cyber security incidents.

The increased likelihood of suffering a security breach means it is essential to put robust incident response plans in place – a point addressed in the fourth objective.

DSPs have the additional requirement of taking business continuity measures to ensure they can resume normal operations as soon as possible if an attack has been successful. That requirement, in combination with ENISA's guidelines, can be met by taking a structured approach to cyber resilience.

Cyber resilience is an approach that recognises that, against the current threat landscape, even the best cyber security methods cannot guarantee the security – and, with it, the functioning – of your operations.

Although not actually a requirement, we recommend that OES also take business continuity measures. As the world becomes increasingly interconnected, being able to respond to an incident quickly is imperative. Even a small glitch can cause revenue loss and have long-term reputational effects.

Additionally, some business contracts require guarantees of organisational resilience, so being able to demonstrate your ability to survive such incidents may also provide new business opportunities.

Full cyber resilience is best achieved via a management system that combines information security and business continuity best practice, while also taking note of best-practice incident response guidelines.

Using a standards-based approach

Article 19 of the Directive states that member states should "encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems".

The NCSC's guidance regularly refers to **ISO/IEC 27002:2013**, the 'code of practice' to **ISO/IEC 27001:2013**, the international standard for an information security management system (ISMS), and to **ISO/IEC 27035:2016**, the international standard for information security incident management. If you are an OES, applying these standards will help you develop tools and processes that are sufficient to meet the Directive's requirements.

If you are a DSP, or an OES aiming for a higher level of maturity – full cyber resilience – the international standard for a business continuity management system (BCMS), **ISO 22301:2012**, can prove valuable.

Using the guidance of all these standards, you will develop a documented cyber resilience framework or a full cyber incident response (CIR) capability that will protect your network and information systems from the majority of threats, and help you recover quickly and efficiently if and when an incident occurs. It will also give your organisation an internationally accepted

posture of cyber resilience based on risk management best practice – exactly as the Directive requires.

ISO 27001 and ISO 27002 – information security

The NIS Directive's incident reporting requirements are not limited to cyber security incidents, but include any incident that affects the security of network and information systems, including physical events.

An ISO 27001-compliant ISMS that draws on the guidance included in ISO 27002 addresses information security risks in all forms, and encompasses people, processes and technology.

It recognises that information security is as much a cultural issue as it is a technological one, and mandates regular risk assessments to ensure the controls you use address the risks you actually face, in accordance with your risk appetite, in line with the Directive's requirement for a "culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced" (Recital 44).

Such a risk-based approach means that resources are deployed efficiently and effectively, staff are regularly trained to be aware of online and offline security threats, such as phishing and other methods of delivering malware, systems are regularly tested to ensure vulnerabilities are patched, and the whole ISMS is regularly audited to demonstrate to investors, stakeholders, customers and staff that information security best practice is being followed as part of everyday operational activities.

ISO 27001 is also the only international standard for information security management against which an organisation can achieve independently audited certification. Such certification can be used to demonstrate to suppliers, stakeholders and the relevant competent authorities that the organisation has taken the "appropriate and proportionate technical and organisational measures to manage the risks posed to the information systems" required.

Meanwhile, ISO 27002 provides comprehensive implementation guidance, building on the structured approach described in ISO 27001.

Penetration testing

A key component of an ISO 27001-compliant ISMS is penetration testing – systematic and controlled probing for vulnerabilities in your applications and networks.

Many cyber attacks can easily be prevented by keeping software and systems up to date. Vulnerabilities are discovered and exploited all the time by opportunistic criminal hackers who use automated scans to identify targets. Closing these security gaps and fixing vulnerabilities as soon as they become known are essential steps to keeping your networks and information systems safe and secure.

Regular penetration testing is the most effective way of identifying exploitable vulnerabilities in your infrastructure, allowing appropriate mitigation to be applied. It would also be good practice to penetration test any new services or networks before making them available.

ISO 27035 – incident response

ISO 27035 outlines concepts, phases and overall guidelines for information security incident management, and can be easily implemented by organisations also aiming to meet ISO 27001's requirements, as many of the two standards' processes line up.

ISO 27035's structured approach to incident response consists of five phases:

1. Plan and prepare
2. Detection and reporting
3. Assessment and decision
4. Responses
5. Lessons learnt

While this approach is approximately in line with general cyber resilience frameworks, it does lack the emphasis on maintaining a minimum acceptable level of business continuity, as well as the focus on returning to full power after an incident. This is not a critical failing, of course, but organisations should be aware of the need to account for these by adopting other processes or standards.

However, ISO 27035 does cover the two main requirements of the Directive – reporting incidents and taking minimum security measures. As such, implementing an ISO 27001-compliant ISMS, and following the guidance of ISO 27035, should provide a solid foundation for an OES to comply with the NIS Directive.

ISO 22301 – business continuity

A BCMS that conforms to ISO 22301 provides a well-defined incident response structure that ensures that when an incident occurs, responses are escalated in a timely manner and the right people take the right actions to respond effectively.

Having robust business continuity measures in place is a requirement for DSPs, and we also strongly encourage OES to consider implementing a BCMS. In addition to protecting your organisation from harm, it could provide you with a competitive advantage and help you comply with other legislation.

Although it is, of course, good business practice to implement a BCMS that covers the entire organisation, for the purposes of NIS Directive compliance, the network is the only thing that will be in scope, so achieving certification to ISO 22301 might not be necessary. However, certification can also lead to new contractual opportunities.

Combining your GDPR and NIS Directive compliance projects

The Directive comes into effect alongside the GDPR,[11] whose requirements will be enshrined in UK law in 2018. This new act will supersede the Data Protection Act 1998.

All organisations in the UK that process personal data – including OES and DSPs – must comply with the requirements of the GDPR by 25 May 2018, or face fines of up to 4% of annual global turnover or €20 million (£17 million) – whichever is greater.

Although it may seem daunting to carry out two major compliance projects over just two years, the overlap in the requirements of the GDPR and NIS Directive means that you will save significant amounts of time and money by combining your projects, especially if you take a standards-based approach to information security.

To get started with a NIS Directive compliance regime, view our range of cyber resilience solutions or our CIR management programme.

Alignment of ISO standards to the NCSC principles

Principle	Guidance
A. Managing security risk Appropriate organisational structures, policies and processes in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services.	ISO 27001 provides a structured approach to information security risk that acts within the scope of an organisation-wide information security policy and ensures the organisation treats information in accordance with legal and regulatory requirements, and in line with business needs.
A.1 Governance Management policies and procedures that define the organisation's approach to securing its network and information systems.	Clause 5 of ISO 27001 establishes the information security policy, which defines the organisation's approach to information security risk management and is approved by top management to ensure oversight from the organisation's top echelons. Clause 5.1.1 of ISO 27002 provides additional guidance on policies for information security.
A.2 Risk management The organisation takes steps to understand and mitigate threats to its network and information systems.	Clause 6 of ISO 27001 provides a structured approach to risk management, taking into account the risks specific to the organisation and the obligations for security and data protection.
A.3 Asset management Assets relevant to network and information systems are determined, understood and protected.	Control category A.8 in Annex A of ISO 27001 relates to asset management, and the related guidance in ISO 27002 provides extensive information on supplementary practices, such as asset ownership, classification and handling.
A.4 Supply chain The organisation asserts its need for cyber resilience throughout its supply chain.	Annex A of ISO 27001 provides a number of relevant controls to support information security through the supply chain, with extensive guidance for each control detailed in ISO 27002. Control A.13.2.2 establishes requirements for information transfer agreements, and control category A.15 relates to supplier relationships generally.
B. Protecting against cyber attack Proportionate security measures in place to protect essential services	A combination of management system processes and information security

and systems from cyber attack or system failures.	controls – informed by risk assessments – protect the organisation's systems and information assets from cyber attacks and other incidents.
B.1 Service protection policies and processes The organisation has policies and procedures for specifically protecting services that help deliver essential services.	Clause 7 of ISO 27001 specifies requirements for critical processes related to managing resources for information security, ensuring appropriate competence and awareness, and establishing requirements for communication and documentation. Meanwhile, Clause 5 of ISO 27002 provides guidance on implementing information security policies, and Clause 7 addresses human resource security at all stages of employment.
B.2 Identity and access control Access systems that support essential services are controlled.	Clause 9 of ISO 27002 contains guidance specific to access control. This includes access control policies, user registration and de-registration, access provision, secure logon procedures, and so on.
B.3 Data security Stored information is protected from incidents that could disrupt essential services.	Clause 8 of ISO 27001 provides the specification for operational planning and control, ensuring that day-to-day operations are appropriately controlled to protect information assets and systems. ISO 27002 provides additional guidance specific to asset management in Clause 8.
B.4 System security Critical systems and technologies are protected from cyber attack.	On the basis of risk assessment, the organisation can apply controls from Annex A of ISO 27001 to mitigate the threat of a cyber attack. This is a reference set of information security controls that can be supported by controls from, for instance, sector-specific control sets.
B.5 Resilient networks and systems Resilience is built into design, implementation, operation and management of systems that support essential services.	Control category A.17 of ISO 27001 outlines controls for the preservation of information security continuity, while ISO 27002 provides further guidance on the information security aspects of business continuity management in Clause 17. In conjunction with an ISO 22301-aligned BCMS, the organisation can maximise its

	resilience and ensure that systems and processes can continue to function despite disruptions and incidents.
B.6 Staff awareness and training Staff are appropriately supported to ensure the security of network and information systems related to essential services.	Clauses 7.2 and 7.3 of ISO 27001 specify the requirements for competence and awareness. The ISO 27001 approach ensures that the organisation's needs are assessed so that adequate training and awareness exercises can be implemented.
C. Detecting cyber security events Appropriate capabilities to ensure network and information system security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services.	Controls for information security fall into three general classes: preventive, detective and reactive. Preventive controls stop incidents from occurring, detective controls identify when an event or incident happens and reactive controls respond to incidents in order to minimise harm. In an ISO 27001 ISMS, detective controls are supported by ongoing information security processes that ensure key risk areas are monitored.
C.1 Security monitoring Potential security problems are identified and security measures are assessed for effectiveness.	ISO 27001 recommends a blended approach to security monitoring that incorporates detective controls, regular auditing and reviews to look for anomalies, and technical approaches such as penetration testing.
C.2 Proactive security event discovery Anomalous events in network and information systems are detected.	This requires a mature approach to event monitoring in order to identify events that may be designed to confound casual monitoring or technological solutions. ISO 27001 promotes an approach to information security that combines people, processes and technologies, which can provide a strong basis for proactively identifying events and incidents.
D. Minimising the impact of cyber security incidents Capabilities to minimise the impacts of a cyber security incident on the delivery of essential services, including the restoration of those services where necessary.	Both ISO 27002 and ISO 27035 provide guidance on incident response, while ISO 22301 provides guidance on continuity. An approach that takes guidance from ISO 27002 and ISO 27035, or all three standards, provides an effective response to cyber security incidents.
D.1 Response and recovery planning	Clause 17 of ISO 27002 provides guidance on planning for and

Suitable incident management and mitigation processes are in place.	implementing information security continuity, while ISO 27035 suggests incident response activities in its fourth phase (Clause 5.5). ISO 22301, meanwhile, provides a specification for a BCMS that uses business impact analysis and risk assessment to determine the most effective way to respond to incidents and disruptions.
D.2 Lessons learned The organisation learns from incidents and implements measures to improve resilience.	Clause 10 of ISO 27001 outlines how the ISMS is continually improved by assessing events and incidents, and analysing what has worked and what has not. Clause 16.1.6 of ISO 27002 also provides guidance on learning from information security incidents in order to best protect the organisation. The fifth phase of ISO 27035 (Clause 5.6) outlines activities that allow an organisation to learn from incidents and make improvements as appropriate. Meanwhile, an ISO 22301-aligned BCMS also implements processes to improve the organisation's resilience by examining events and incidents, and incorporating the lessons learned into the business continuity plan.

IT Governance products and services

IT Governance is an information security, governance, risk management and compliance specialist, with more than 15 years' experience helping organisations of all sectors and sizes all over the world.

We provide a complete service, including books, standards, documentation toolkits, software, training, consultancy and technical services. We've led more than 400 successful ISO 27001 certification projects alone, and offer a 100% guarantee of certification.

Please see below for more information on how we can help you meet your NIS Directive compliance needs.

- **Consultancy**
  Organisations can demonstrate that they have applied the measures required by the NIS Directive by implementing an organisational cyber resilience programme that combines information security standards. For a higher level of cyber resilience, OES should incorporate business continuity measures.

  Drawing on our unique blend of practical information security know-how and proven management system consultancy expertise, our team will help you implement a framework that combines the requirements of the international standards ISO 27001 and ISO 22301.

Cyber Health Check	Identify your weakest security areas and understand how to take appropriate measures to mitigate your risks and transform your cyber security stance.
Cyber Essentials	Prevent up to 80% of cyber attacks, with certification to demonstrate you have implemented basic cyber security controls.
Information security management and ISO 27001 compliance	Apply organisation-wide protection of all your information: protect the confidentiality, integrity and availability of your data, reduce costs and improve your cyber resilience posture.
Penetration testing	Accurately evaluate your organisation's ability to protect its networks, applications, endpoints and users from determined attackers: get detailed information on actual, exploitable security threats, prioritise remediation, apply necessary security patches and allocate security resources.
Cyber incident response consultancy	Detect cyber incidents at an earlier stage and develop an effective defence against the attack.
Business continuity management and ISO 22301 compliance	Continue to provide a minimum acceptable service if you have been affected by a cyber attack, helping preserve your corporate reputation and minimise losses.

- **Documentation toolkits**
  Creating documentation for your management system is never easy, and can run to hundreds of pages. IT Governance's documentation toolkits contain fully customisable templates that have been written by our consultants to comply with international standards:

    - **Cyber resilience**
      Combining our bestselling ISO 27001 ISMS and ISO 22301 BCMS toolkits, the Cyber Resilience Toolkit accelerates your route to a cyber resilient posture, helping you stay ahead of the game.

    - **ISO 27001**
      The ISO 27001 ISMS Documentation Toolkit provides you with a comprehensive set of pre-written ISMS documents that comply with ISO/IEC 27001:2013.

    - **ISO 22301**
      The ISO 22301 BCMS Implementation Toolkit contains expert guidance and consultant-created content to help you implement an ISO 22301-compliant BCMS quickly and easily, and mitigate the effects of unplanned business disruptions.

- **Training**
  IT Governance's training programme is built on the foundations of our extensive practical experience designing and implementing management systems. Our training courses offer a structured learning path from Foundation to Advanced level for IT practitioners and lead implementers, and help to develop the skills needed to deliver best practice and compliance in any organisation.

    - The ISO 27001 learning pathway will equip you with the knowledge and skills required to plan, implement, maintain and audit a best-practice ISMS in your organisation.

    - The ISO 22301 learning pathway provides attendees with the knowledge and skills to implement and audit an ISO 22301-compliant BCMS.

    - The Incident Response Management Foundation Training Course helps attendees effectively manage and respond to a disruptive incident and take appropriate steps to limit the damage of a disruption to network availability and information security.

    - The intensive five-day Certified Cyber Resilience Practitioner Training Course helps attendees learn how to identify, detect, respond to and recover from a cyber attack.

  Attendees who pass the included examinations will be awarded certificates from GASQ and the International Board for IT Governance Qualifications (IBITGQ).

IT Governance: for all your NIS Directive compliance needs.

Contact us: +44 (0)333 800 7000
www.itgovernance.co.uk servicecentre@itgovernance.co.uk

Appendix

Table of essential services and identification thresholds

Sector	Subsector	Essential service	Identification thresholds
Drinking water supply and distribution	N/A	The supply of potable water to households.	Operators with sites serving 200,000 or more people.
Energy	Electricity	The function of supply (the sale or resale of electricity) to consumers.	In England, Scotland and Wales: Electricity suppliers (including aggregators where they act as suppliers) that meet the following two criteria (both must apply): • Use of smart metering infrastructure. • Supply > 250,000 consumers. Operators of electricity generators* with a generating capacity ≥ 2 gigawatts (GW), including: • Standalone transmission connected generation; and • Multiple generating units with a cumulative capacity ≥ 2GW controlled by an individual/common control network. *Excluding nuclear electricity generation. The government does not consider the civil nuclear sector to be in scope of the NIS Directive. In Northern Ireland: Licensed suppliers that supply to > 8,000 customers. And any generator with a generating capacity ≥ 350MW.

		Electricity (SEM operator).	The holder of a SEM operator licence under Article 8(1)(d) of the Electricity (NI) Order 1992.*
		Electricity (transmission).	In England, Scotland and Wales: Network operators with the potential to disrupt supply to > 250,000 consumers. International interconnectors and DC converter station with a capacity ≥ 1GW. In Northern Ireland, holders of a transmission licence under Article 8(1)(b) of the Electricity (NI) Order 1992.
		Electricity (distribution).	In England, Scotland and Wales: Network operators with the potential to disrupt supply to > 250,000 consumers. In Northern Ireland, holders of a distribution licence under Article 8(1)(bb) of the Electricity (NI) Order 1992.
	Oil	Oil transmission (upstream).	Operators with throughput of more than 20 million barrels of oil equivalent (BOE) of oil per year.
		Oil transmission (downstream). The distribution of petroleum-based fuels to other storage sites throughout the UK by road, pipeline, rail or ship.	In England, Scotland and Wales: Operators that provide or handle 500,000 tonnes of fuel per year. In Northern Ireland, operators that provide or handle 50,000 tonnes of fuel per year.
		Oil production, refining and treatment and	Operators with throughput of 20 million BOE of oil per year.

		storage (upstream).	
		Oil production, refining and treatment and storage (downstream). – The import of any of crude oil, intermediates, components and finished fuels. – The storage of any of crude oil, intermediates, components and finished fuels. – The production of intermediates, components and finished fuels through a range of refining or blending processes. – The distribution of petroleum-based fuels to other storage sites throughout the UK by road, pipeline, rail or ship. – The delivery of petroleum-based fuels to retail sites, airports or end users.	In England, Scotland and Wales: Operators that provide or handle 500,000 tonnes of fuel/per year. In Northern Ireland, operators that have a storage capacity > 50,000 tonnes of fuel.
	Gas	The function of supply (the sale or resale of gas) to consumers.	In England, Scotland and Wales: Gas suppliers (including aggregators where they act as suppliers) that meet the following two criteria (both must apply):

			• Use of smart metering infrastructure. • Supply > 250,000 consumers. In Northern Ireland, licensed suppliers that supply to > 2,000 customers.
		Gas (transmission) (downstream).	In England, Scotland and Wales: Network operators with the potential to disrupt supply to > 250,000 consumers. Operators of gas interconnectors with technical capacity > 20mcm/d. In Northern Ireland, holders of a licence under Article 8(1)(a) of the Gas (NI) Order 1996.
		Gas (distribution).	In England, Scotland and Wales: Network operators with the potential to disrupt supply to > 250,000 consumers. In Northern Ireland, holders of a licence under Article 8(1)(a) of the Gas (NI) Order 1996.
		Gas storage facilities supplying/storing gas for the national transmission network.	In England, Scotland and Wales: Operators with the potential to input > 20mcm/d to the national transmission network. In Northern Ireland, holders of a licence under Article 8(1)(b) of the Gas (NI) Order 1996.
		LNG system operators supplying/storing gas for the national transmission network.	In England, Scotland and Wales: Operators with the potential to input > 20mcm/d to the national transmission network. In Northern Ireland, holders of a licence under Article 8(1)(d) of the Gas (NI) Order 1996.

		Gas (transmission) (upstream).	Operators with throughput of more than 20 million BOE of gas per year.
		Gas (production, refining and treatment)	Operators with throughput of more than 20 million BOE of gas per year.
Digital infrastructure	N/A	Top-level domain (TLD) name registries.	Operators that service an average of 2 billion queries or more in 24 hours for domains registered within ICANN. Note: this threshold is an annual average and shall be based on the best available data from the preceding 12 months. Note: the threshold excludes growth of traffic load due to malicious activity such as distributed denial-of-service attacks.
		Domain name services (DNS) service providers.	Operators that provide DNS resolution and which service an average of 2 million queries or more in 24 hours. Operators that provide authoritative hosting of domain names, offered for use by publicly accessible services, servicing ≥ 250,000 different domain names. Note: this threshold is an annual average and shall be based on the best available data from the preceding 12 months.
		IXP operators.	Operators that have ≥ 50% annual market share among UK IXP operators in terms of interconnected autonomous systems, or that offer interconnectivity to ≥ 50% of global Internet routes. Note: 'interconnected autonomous system' is defined in NIS Directive Article 4 (13).

			Note: 'global Internet route' means: the total number of active entries within the Global Internet Routing Table, averaged per calendar year.
Health sector	Healthcare settings	Healthcare services.	In England: Providers of non-primary NHS healthcare commissioned under the National Health Service Act 2006 as amended in England (but not including any individual doctors providing such healthcare). In Wales: Local health boards and NHS trusts (defined by the National Health Service (Wales) Act 2006). In Scotland: The 14 territorial health boards; the following four special NHS boards: NHS National Waiting Times Centre, NHS24, Scottish Ambulance Service and The State Hospitals Board for Scotland; and Common Services Scotland (known as NHS National Services Scotland). In Northern Ireland: Health and social care trusts (defined by Health and Social Care (Reform) Act (Northern Ireland) 2009).
Transport	Air transport	Owner or operator of an aerodrome (as defined in the Civil Aviation Act 1982).	Owner or operator of any aerodrome (i.e. airport) with annual terminal passenger numbers greater than 10 million.
		Provider of air traffic services (as defined in the Transport Act 2000).	Any entity that is licensed to provide UK en route air traffic services. Air traffic service providers at airports with annual terminal passenger numbers greater than 10 million.
		Air carriers (as defined in paragraph 4 of	Air carriers with more than 30% of the annual terminal passengers at any individual UK airport that is in scope of

		Article 3 of Regulation (EC) No 300/2008).	the Directive and more than 10 million total annual terminal passengers across all UK airports.
	Maritime transport	Harbour authorities (as defined in the Merchant Shipping Act 1995). Operators of vessel traffic services (as defined in the Merchant Shipping (Vessel Traffic Monitoring and Reporting Requirements) Regulations 2004 SI 2004/2110).	Harbour authorities or operators at ports with annual passenger numbers > 10 million. Or at ports that account for: • 15% of UK total Roll on-Roll off (Ro-Ro) traffic; • 15% of UK total Lift on-Lift off (Lo-Lo) traffic; • 10% of UK total liquid bulk; or • 20% of UK biomass fuel.
		Operators of a port facility (as defined in the Port Security Regulations 2009 – SI 2009/2048).	Operators of port facilities at ports that meet the above thresholds and that handle the type of freight specified in those thresholds.
		Passenger and freight water transport companies (as defined for maritime transport in Annex I to Regulation (EC) No 725/2004).	Operators that handle more than 30% of the freight at any individual UK port that is in scope and more than 5 million tonnes of total annual freight at UK ports. Operators that have more than 30% of the annual passenger numbers at any individual UK port that is in scope and more than 2 million total annual passengers at UK ports.
	Rail transport	Operators of any railway asset (as defined in section 6 of the Railways Act 1993) on the	Any operator of a railway asset on the mainline railway network (as defined).

		mainline railway network. This will include operators of trains, networks, stations and light maintenance depots, where operating those assets on the mainline railway network. Railway undertaking as defined in the Northern Ireland Transport Act 1967. The mainline railway network will be defined to include all railways in GB but will exclude: i. International rail; ii. Metros, trams and light rail systems; iii. Heritage, museum or tourist railways whether or not they are operating solely on their own network; and iv. Networks that are privately owned and exist solely for use by the infrastructure owner for its own freight	

		operations or other activities not involving passenger or freight services for third parties.	
		Operators of railway assets (as defined in section 6 of the Railways Act 1993) for metros, trams and light rail (including underground) systems.	Operators with annual passenger journeys greater than 50 million.
		Operators of international rail services.	Any operator of a Channel Tunnel train (as defined in the Channel Tunnel Security Order 1994). Any operator of international rail services in Northern Ireland, as defined in the Northern Ireland Transport Act 1967.
		International rail infrastructure managers.	Any infrastructure manager of the Channel Fixed Link, i.e. the Concessionaires (as defined in the Channel Tunnel Act 1987). Any infrastructure manager of international rail services in Northern Ireland, as defined in the Northern Ireland Transport Act 1967.
	Road transport	Road authorities as defined in point (12) of Article 2 of the Commission Delegated Regulation (EU) 2015/962.	A road authority responsible for roads in the United Kingdom that annually in total have vehicles travelling > 50 billion miles on them.
		Operators of intelligent	A road authority that provides an intelligent transport systems service

		transport systems as defined in point (1) of Article 4 of Directive 2010/40/EU of the European Parliament and of the Council.	that covers roads in the UK that annually in total have vehicles travelling > 50 billion miles on them.

[1] European Commission, "EU Cybersecurity plan to protect open internet and online freedom and opportunity", February 2013, http://europa.eu/rapid/press-release_IP-13-94_en.htm.
[2] Department for Digital, Culture, Media and Sport, "Security of Network and Information Systems: Government response to public consultation", January 2018, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/677065/NIS_Consultation_Response_-_Government_Policy_Response.pdf.
[3] Micro and small enterprises are defined by the European Commission in 2003/361/EC, which states that "a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million", and that "a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million".
[4] "Security of Network and Information Systems: Government response to public consultation".
[5] Commission Implementing Regulation (EU) 2018/151.
[6] Department for Digital, Culture, Media and Sport, "Security of Network and Information Systems Targeted consultation on Digital Service Providers", March 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/694290/DSP_Targeted_Consultation__Final_.pdf.
[7] ENISA, "Technical Guidelines for the implementation of minimum security measures for Digital Service Providers", February 2017, https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers.
[8] ICO, "The Information Commissioner's comments on the European Commission publication of the Commission Implementing Regulation pursuant to Art 16(8) of the NIS Directive (EU 2016/1148)", October 2017, https://ico.org.uk/media/about-the-ico/consultation-responses/2017/2172540/ico-response-ec-nis-directive-implementing-regs-consultation.pdf.
[9] Department for Digital, Culture, Media and Sport, "Security of Network and Information Systems Targeted consultation on Digital Service Providers", March 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/694290/DSP_Targeted_Consultation__Final_.pdf.
[10] NCSC, Table view of principles and related guidance, March 2018, https://www.ncsc.gov.uk/guidance/table-view-principles-and-related-guidance.
[11] Regulation (EU) 2016/679.