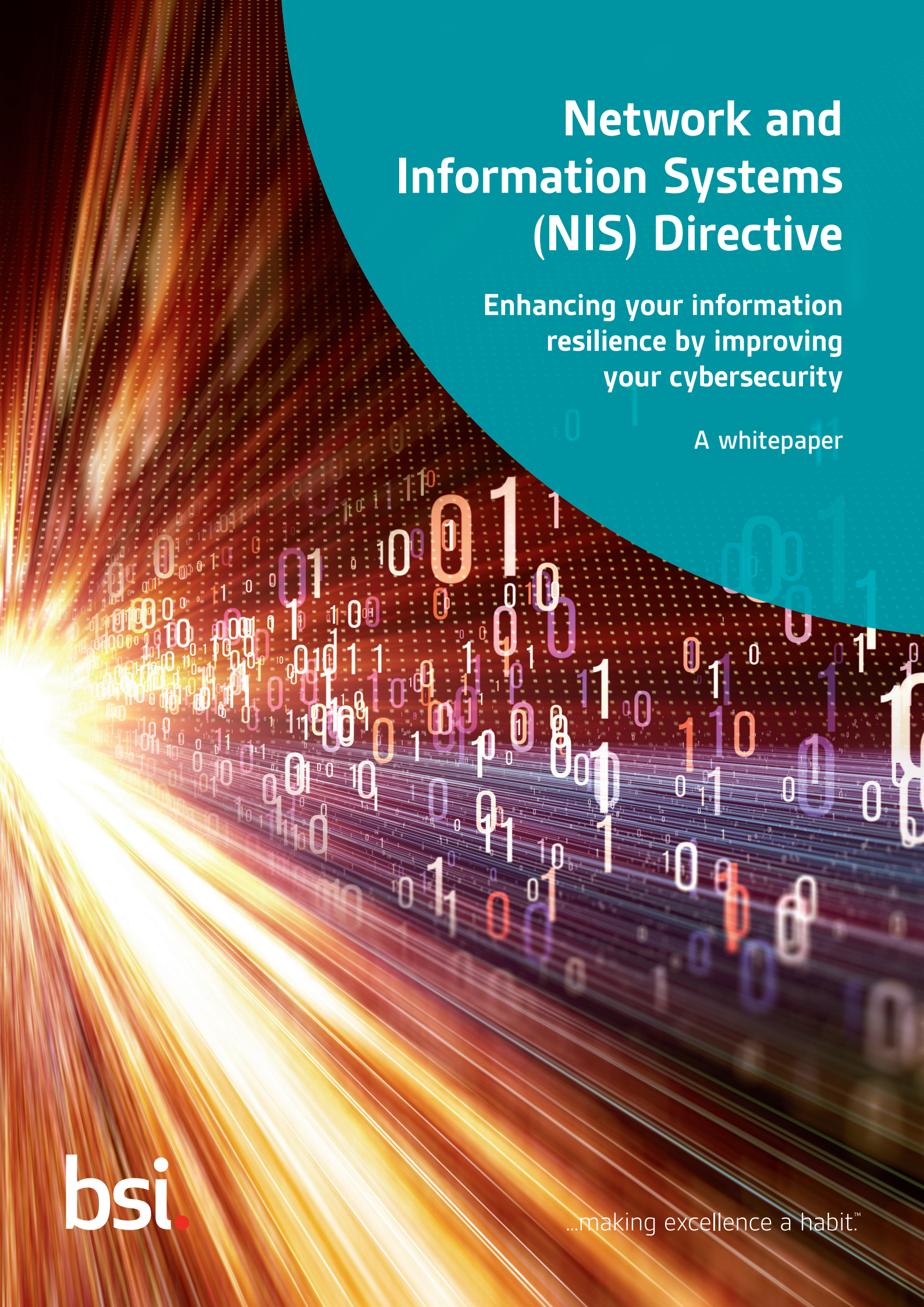


Network and Information Systems (NIS) Directive

Enhancing your information resilience by improving your cybersecurity

A whitepaper

bsi.

...making excellence a habit.™

Introduction

"Continually enhancing your organization's state of information resilience protects your business, people, stakeholders and reputation. This requires the adoption of security minded practices enabling information to be generated, stored and accessed securely, efficiently and effectively."

Michael Bailey, EMEA Director of Professional Services, BSI Cybersecurity and Information Resilience

To achieve a state of information resilience, organizations must address four interconnecting sub-domains:

1. **Cybersecurity**
2. **Information management and privacy**
3. **Security awareness and training**
4. **Compliance to requirements**

The NIS Directive was adopted by the European Parliament in 2016 and became law in all member states including the UK in 2018. The purpose of the NIS Directive is to improve the cybersecurity capabilities of EU member states at a national level

This whitepaper will explore the tenets of the NIS Directive, the importance of the mandate, why organizations should adopt these protocols, how to implement a cyber assessment framework model and moreover, achieve an enhanced and sustainable state of information resilience.

Is the NIS Directive on your radar?

Almost every organization today relies on networks and information systems. These systems are subject to adverse security threats arising from technical failure, unintentional human error or deliberate malicious attack.

The exploitation of such threats could significantly affect the supply of essential services that we rely on in our daily lives including electricity, transport, water, energy, health and digital infrastructure. Any disruption to these services – collectively known as Critical Infrastructure – would affect citizens, markets and economic stability.

The Network and Information Systems (NIS) Directive is the first piece of EU-wide legislation relating to cybersecurity. It places legal obligations on all providers of Critical Infrastructure to ensure that they are prepared to deal with the increasing volume of cyberthreats and as mentioned, was adopted by the European Parliament in 2016, becoming law in all member states including the UK in 2018.

Purpose of the NIS Directive

At a member state level, the NIS Directive is designed to secure critical infrastructure from cybersecurity threats by focusing on the three top-level objectives:

Improved cybersecurity capabilities at national level

- All EU member states must adopt a national strategy for the security of network and information systems. The NIS strategy contains the objectives and frameworks under which the relevant regulatory measures will be enacted and monitored.
- EU member states need to have at least one designated National Competent Authority, which is responsible for monitoring the application of the NIS Directive at a national level. There must also be a Single Point of Contact (SPOC) to ensure cross border cooperation among member states. In addition to the SPOC, member states must have at least one Computer Security Incident Response Team (CSIRT) with responsibility for monitoring and responding to incidents at a national level.
- The roles of the SPOC and CSIRT have been taken on by the respective National Cyber Security Centres in the UK and Ireland.

Increased level of EU cooperation

- A cooperation group was established to facilitate the exchange of information among EU member states. This group comprises representatives of member states, the EU Commission and the European Union Agency for Network and Information Security (ENISA).

Supervision of critical sectors

- According to the NIS Directive, all EU member states must supervise the cybersecurity of their critical market operators. These include operators of essential services (transport, energy, water, health, financial sector) and digital service providers (online marketplaces, online search engines, cloud computing services).

Who does the NIS Directive apply to?

The NIS Directive applies directly to Operators of Essential Services (OES) and Digital Service Providers (DSP).

Operators of Essential Services (OES)

The NIS Directive places legal obligations on all operators of essential services including energy, banking, transport, water, health, financial markets and digital infrastructures. The role of identifying operators of essential services has been taken up primarily by incumbent regulatory bodies for those sectors.

In addition, the regulatory authority per each sector will have contacted the relevant essential services organizations whom are subject to the NIS Directive and will be looking for them to provide evidence of how they comply with the directive.

Digital Service Providers (DSP)

DSPs must self-register with their competent authority and determine whether they are an in-scope digital service provider. A good way to determine this is to question the impact to a member state if you were to cease operations tomorrow:

1. Would there be a material impact to the country?
2. Do you provide a critical service to an OES?

The UK's Information Commissioner's Office (ICO) has also provided guidance in this area to help organizations determine their status. A DSP is likely to be subject to the NIS directive where they:

- provide one or more of the following digital services: an online search engine, an online marketplace, and a cloud computing service; or
- has a head office is in the UK, or has nominated a UK representative; and
- employ more than 50 staff and a turnover or balance sheet of more than €10 million.

Requirements for OES and DSPs

As incumbent and primary stakeholders of the NIS Directive, OES and DSP have numerous requirements.

Firstly, at an operational level, they must take appropriate and proportionate technical and organizational measures to manage risks to network and information systems that are used to provide essential services.

Subsequently, they must prevent and minimize the impacts of any incidents that affect these same networks and information systems, with a view to ensuring continuity.

Lastly but just as importantly, providers of essential services must, without undue delay, alert the relevant competent authority or CSIRT no later than 72 hours after they have become aware of an incident.

These alerts or notifications must contain enough information to enable authorities to determine the cross-border impact of the incident.

The table below summarizes some key information for incident reporting focusing on the UK and Ireland. Organizations should understand their obligations in respect of the directive pointed out above.

It is also worth noting that fines are primarily intended to be levied where the incident management process has failed or where entities fail to engage with component authorities.

Incident management overview for OES and DSP		
	UK	**Ireland**
Competent Authority (CA)	OES – Per Sector DSP – Information Commissioners Office (ICO)	OES – Per sector DSP – Minister for Communications
Incident Classification	• Risk based • Consider notification where a breach leads to impact to the continued good operation of an essential service. Variables include: › nature of the service, number of people and size of region effected, whether the breach may affect the economy or poses a threat to life.	
Incident Notification	Without undue delay < 72 hours	Without undue delay < 72 hours
Sanctions	Up to £17m[1]	Up to €500k
Approach	Cyber Assessment Framework (CAF)	NIST Cyber Security Framework US Federal Standards

Fig 1 - Key information for incident reporting focusing on the UK and Ireland. 1The £17m fine is intended to be applied where a breach may result in a threat to life or significant threat to the UK economy.

Application of cybersecurity – which framework to choose?

Each member state has the option to implement appropriate cybersecurity frameworks as they see fit. However, a significant number of member states have opted to align themselves with suitable frameworks such as:

1. UK National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) (see more details on page 8). In support of the UK NIS Directive implementation, the NCSC is committed to working with lead government departments, regulators and industry to develop a systematic method of assessing the extent to which an organization is adequately managing cybersecurity risks in relation to the delivery of essential services. This assessment method, otherwise known as the Cyber Assessment Framework (CAF), is intended to meet both NIS Directive requirements and wider CNI needs.
2. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.
(Ref: nist.gov/cyberframework)

A Juxtaposition – Comparing the NCSC CAF and the NIST CSF

The NCSC Cyber Assessment Framework

Objective A Managing security risk	**Objective B** Protecting against cyber - attack
Objective C Detecting cyber events	**Objective D** Minimising the impact of cyber events

The NIST Cybersecurity Framework

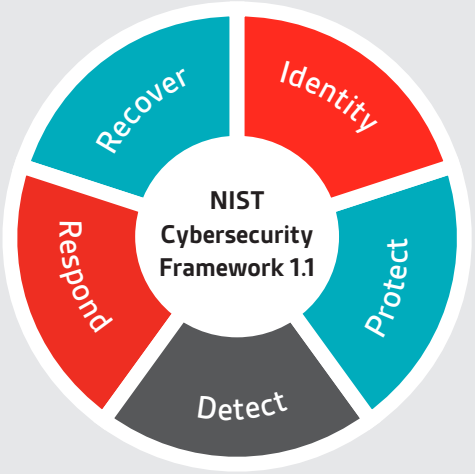


Fig 2 - Comparing the NCSC Cyber Assessment Framework and the NIST Cybersecurity Framework

As Fig 2 shows there are clear overlaps between the two frameworks, although the NCSC CAF has structured its framework as an objective-based assessment. When the NCSC CAF and NIST CSF are compared, the overlap becomes even more pronounced. Taking the "Identify" section of the NIST CSF (top right) and the Object A of the NSCS (top left), they both cover the following and cross over where **highlighted**. This sequence and marriage between the two is evident throughout the vast majority of the frameworks.

NCSC CAF
Objective A: Managing Security Risk

- Governance
- Risk Management
- Asset Management
- Supply Chain

NIST CSF
Segment: Identify

- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management
- Asset Management
- Business Environment

Fig 3 - Comparing NCSC CAF Objective A and NIST CSF Identify segment

Complying with the NIS Directive

Article 19 of the NIS Directive encourages "*the use of European or internationally accepted standards and specifications relevant to the security of network and information systems*".

International security standards such as ISO/IEC 27001:2013 (the international standard for an Information Security Management System), ISO/IEC 27002:2013 (the 'code of practice') and the NIST (National Institute of Standards and Technology) Cyber Security Framework serve as a framework for organizations aiming to comply with the NIS Directive.

In addition to ISO/IEC 27001 and ISO/IEC 27002, there are other standards such as ISO/IEC 27035 (Information Security Incident Management), ISO 22301 (Business Continuity Standard) and COBIT 5 that can help organizations achieve a cyber resilience framework and protect network / information as per the NIS Directive requirements.

The role of UK National Cybersecurity Centre (NCSC)

The NCSC provides technical support and guidance to the OES, competent authority and other government departments. The three main support roles provided by the NCSC are:

1. Acting as a Single Point of Contact (SPOC) for all EU engagements from coordination to submitting annual incident statistics.
2. Advising organizations that have experienced an incident by acting as a CSIRT (Computer Security Incident Response Team).
3. Providing technical expertise in the field of cybersecurity for OES and CAs.

Exploring the NCSC Cyber Assessment Framework (CAF)

In 2018, the NCSC published the first version of the CAF as part of the implementation of the EU security of Networks and Information Systems (NIS) Directive.

The CAF enables NIS regulatory bodies (known as Competent Authorities) to assess the cybersecurity of organizations covered by the Directive. The CAF below outline the four pillars of the NIS Directive which are underpinned by 14 principles, with a list of definitions – and how each objective is applied – underneath.[2]

NIS Objectives							
A: Managing Security Risk		**B: Protecting Against Cyber-attack**		**C: Detecting Cybersecurity Incidents**		**D: Minimizing The Impact Of Cybersecurity Incidents**	
NIS Principles							
A1: Governance	A2: Risk Management	B1: Service Protection and Policies and Processes	B2: Identity and Access Control	C1: Security Monitoring	C2: Proactive Security Event Discovery	D1: Response and Recovery Planning	D2: Lessons Learned
A3: Asset Management	A4: Supply Chain	B3: Data Security	B4: System Security				
		B5: Resilient Network and Systems	B6: Staff Awareness and Training				

Fig 4 - Cyber Assessment framework v2.0 objectives and principles , [2] Ref : https://www.ncsc.gov.uk/blog-post/introducing-cyber-assessment-framework-v20

Objectives	Principle
A: Managing Security Risk	**Governance:** There are appropriate management policies and processes in place to govern the organization's approach to the security of network and information systems.
	Risk Management: The organization takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the delivery of essential services. This includes an overall organizational approach to risk management.
	Asset Management: All systems and/or services that are required to maintain or support essential services are determined and understood. This includes data, people and systems as well as any supporting infrastructure such as power.
	Supply Chain: The organization understands and manages security risks to networks and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where 3rd party services are used.
B: Protecting Against Cyber-attack	**Service Protection Policies and Processes:** The organization defines and communicates appropriate policies and processes that direct the overall organizational approach to securing systems and data that support delivery of essential services.
	Identity and Access Control: The organization understands, documents and controls access to systems and functions supporting the delivery of essential services. Rights or access granted to specific users or functions should be understood and managed.
	Data Security: The organization prevents unauthorized access to data whether through unauthorized access to user devices, interception of data in transit or accessing data remaining in memory when technology is sent for repair or disposal.
	Other – System Security, Resilient Networks and Staff Awareness & Training: The organization ensures that the network and information systems are protected from cyber-attacks by managing all security controls and building resilience. The organization also safeguards staff and provides appropriate support to ensure they can maintain the security and resilience of the systems and networks.
C: Detecting Cybersecurity Incidents	**Security Monitoring:** The organization monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and track the ongoing effectiveness of protective security measures.
	Anomaly Detection: The organization detects anomalous events in the network and information systems affecting, or with the potential to affect, the delivery of essential services.
D: Minimizing The Impact Of Cybersecurity Incidents	**Response and Recovery Planning:** There are well-defined and tested incident management processes in place that aim to ensure continuity of essential services in the event of system or service failure. Mitigation activities are in place that are designed to contain or limit the impact of compromise.
	Lessons Learned: When an incident occurs, steps must be taken to understand the root cause of that incident and take appropriate action.

Fig 5 - Cyber Assessment framework v2.0 explained. Ref : https://www.ncsc.gov.uk/blog-post/introducing-cyber-assessment-framework-v20

NIS Directive: A case study

How BSI enhanced and optimized a large utility provider's readiness for the EU NIS Directive implementation.

Requirements

BSI's Cybersecurity and Information Resilience team (CSIR) was asked by an OES in the energy sector to conduct an initial gap analysis against the upcoming EU NIS Directive requirements, based on the guidelines provided by the UK's NCSC, with the intention of laying the groundwork for a risk and maturity assessment.

Challenges

While it was clear that the organization had many strong security controls in place, actions for improvements were identified in the areas of incident management and web gateway security.

Incident management processes were in place, however they were not at the level of maturity expected for an operator of essential services due to lack of intrusion detection capabilities and fit for purposes response processes to handle a security event.

Visibility of web gateway activity was also an issue in the organization, with decentralized and inconsistently applied policies across the estate, resulting in unmanaged access to the internet.

Fig 6 - Initial gap analysis. It's an example only, not real data.

Solutions

With a thorough understanding of the client's requirements, BSI's security experts provided both consultancy and implementation to achieve the desired results.

This engagement was carried out using a structured approach with standard BSI client engagement methodology. Fig 6 shows the assessment that enables the creation of the customer's road map towards meeting their goals.

Scoping workshop

BSI consultants initiated the engagement in a kick-off workshop, bringing together key stakeholders to determine the scope, gather information, and plan assessment activities.

Assessment and roadmap

Following the scoping workshop, BSI undertook a gap analysis against the UK CAF to determine the "as is" position and maturity of controls, providing coverage on a representative sample of in scope systems. This exercise provided a full assessment of the 'as is' activities and results in maturity determination and a detailed report and roadmap to compliance.

Support

BSI supported the OES by leveraging a comprehensive set of products, services and experienced consultants, to develop policies and work with the technical teams to embed appropriate and proportionate security measures into business as usual. BSI provided expertise in configuring secure web filtering and driving increased incident response maturity though the simulated table top and purple team exercises.

In addition to the services outlined in this case study, the table below further describes the services BSI provides aligned with the NCSC CSF and the sub-domains of Information Resilience:

1. Cybersecurity
2. Information management and privacy
3. Security awareness and training
4. Compliance to requirements

The color coded rows on top identify the services within the sub-domains of Information Resilience. The 14 principles of the NIS directive are then shown in the rows below indicating the relevant services by column.

Cybersecurity Services		Cloud Security Solutions	Vulnerability Management	Incident Management	Penetration Testing / Red Teaming	Virtual CISO	TP Security / Risk Assessment
Information Management & Privacy		eDiscovery eDisclosure	Digital Forensics	Legal Tech	Data Protection Services	Data Subject Requests	DPO as a service
Security Awareness & Training		End User Awareness	Phishing Simulations	Social Engineering	Certified Info Sec Training	Onsite and Bespoke Training	Online Interactive Solutions
Compliance services		PCI DSS	NIST	ISO 27001 Implementation	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	● ● ● ●	● ● ● ●	● ● ● ●	● ● ● ●	● ● ● ●	● ● ● ●

Fig 7 - The type of BSI services that address each 14 principles of the NIS Directive.

Conclusion

As has been evident throughout this whitepaper, compliance with requirements and regulations, including directives, is paramount to the sustainability and longevity of any organization. This requires the adoption of security minded practices enabling information to be generated, stored and accessed securely, efficiently and effectively.

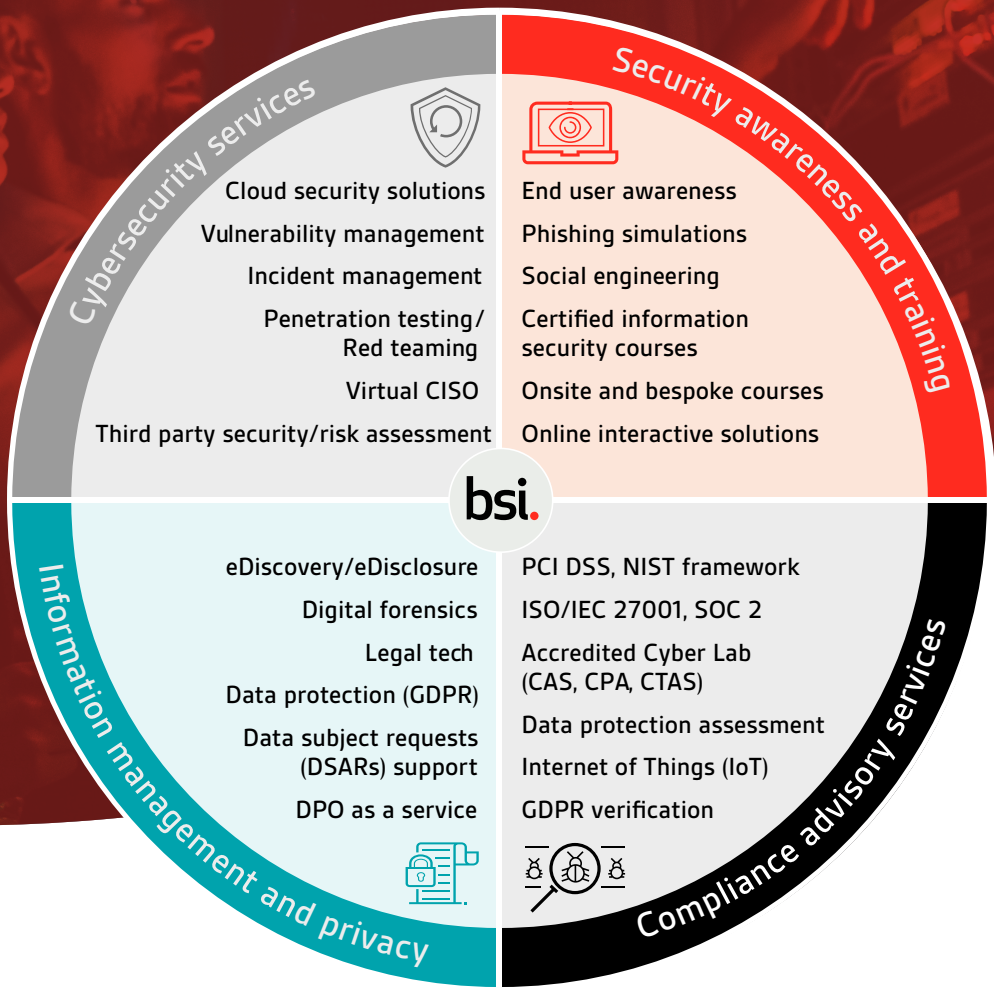
With the ever-increasing growth of cyber-attacks, employing the tenets of the NIS Directive is imperative. A prevention-only based cybersecurity strategy is not enough, you must plan for resilience through rapid detection and practiced response.

Governments and countries are now taking note and making changes in how cybersecurity and risk are being managed, implemented and maintained. The NIS Directive gives organizations as part of the critical national infrastructure (CNI) the opportunity to deploy best practice cybersecurity protocols. As outlined, there are many frameworks that can be used, including the important and mature UK NCSC cyber assessment framework (CAF). This framework nurtures sustainability, mitigates risk, protects organizations, their information, safeguards their people and ensures a state of enhanced information resilience. A resilient organization is not one that merely survives over the long term but flourishes – passing the test of time.

BSI Cybersecurity and Information Resilience

Protecting your information, people and reputation

BSI Cybersecurity and Information Resilience helps you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that affect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:



Our expertise is accredited by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CYBER ESSENTIALS

CREST STAR

CHECK IT Health Check Service

Find out more

bsi.

UK

Call: +44 345 222 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com

IE/International

+353 1 210 1711
cyber.ie@bsigroup.com
bsigroup.com