tripwire

WHITE PAPER

How to Achieve Compliance with the NIS Directive and NIS Regulations

Anastasios Arampatzis

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Network and information systems (NIS) and the essential functions they support play a vital role in society from ensuring the supply of electricity, water, oil and gas to the provisioning of healthcare and the safety of passenger and freight transport. In addition, computerized systems are performing vital safety-related functions designed to protect human lives. For example, such systems are controlling the safe operation of industrial sites that process and store dangerous chemicals as well as those that play a key role in the safety of aviation, rail transportation etc. Their reliability and security are essential to everyday activities.

As we have seen from numerous cybersecurity incidents, these systems can be an attractive target for malicious actors, and they can also be susceptible to disruption through single points of failure. The magnitude, frequency and impact of network and information system security incidents are increasing. Events such as the **2017 WannaCry ransomware attack**, the 2016 attacks on U.S. water utilities, and the **2015 attack on Ukraine's electricity network** clearly highlight the impact that incidents can have.

Computerized safety systems could be adversely affected by a cyber incident either as a side-effect of a compromise or as a result of a highly targeted cyber-attack that's specifically aimed at reducing the effectiveness of safety mechanisms. Such was the case with **TRITON malware**.

Cyber incidents can result in several different consequences depending on the nature of the computer systems targeted and the intention of the perpetrators. Given that the possible consequences of cyber incidents can be extremely serious or perhaps even catastrophic, industrial organizations require very robust levels of cybersecurity and resilience.

There is, therefore, a need to improve the security of network and information systems. Those efforts should especially focus on essential functions which if compromised could potentially cause significant damage to the economy, society, the environment, and individuals' welfare, including loss of life.

For the reasons above, the European Union has taken the lead and developed the **Directive on Security of Network and Information Systems (NIS Directive),** enacted in the United Kingdom as **The Network and Information Systems Regulations 2018 (NIS Regulations)**, which aims to raise levels of cybersecurity and resilience of key systems across the EU and United Kingdom.

What is the NIS Directive?

According to the NIS Directive, member states should adopt a common set of baseline security requirements to ensure a minimum level of harmonized security measures across member states and to enhance the overall level of security of operators providing essential services (OES) and digital service providers (DSP) in the EU and UK.

The NIS Directive sets three primary objectives:

- To improve the national information security capabilities of the member states
- To build mutual cooperation
- To promote a culture of risk management and incident reporting among actors (OES and DSP) of particular importance for the maintenance of key economic and societal activities in the Union.

The NIS Directive provides the legal footing to:

- Ensure that member states have in place a national framework so that they are equipped to manage cybersecurity incidents and oversee the application of the directive. This includes a National Cyber Security Strategy, a Computer Security Incident Response Team (CSIRT), and a National Competent Authority (NCA), or competent authorities
- Set up a Cooperation Group among member states to support and facilitate strategic cooperation and the exchange of information. The member states participate in a CSIRT Network to promote swift and effective operational cooperation on specific network and information system security incidents as well as sharing information about risks.
- Ensure that organizations within vital sectors which rely heavily on information networks, for example, utilities, healthcare, transport, and digital infrastructure sectors, are identified by each member state as

The Network and Information Systems Regulations 2018 (NIS Regulations)

The United Kingdom has enacted The Network and Information Systems Regulations 2018 (NIS Regulations), equivalent to the NIS Directive, and subject to Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019, which amend the NIS Regulations to

- Remove certain obligations from the NCSC regarding international cooperation;
- Remove references to EU-based service providers; and
- Convert euros to sterling.

For the purposes of this paper, the two acts will simply be referred to as the NIS Directive, and any reference to "member states" generally applies to the UK as well.

"operators of essential services" (OES). Those OES are required to take appropriate and proportionate security measures to manage risks to their network and information systems, and they are required to notify serious incidents to the relevant national authority. The participation of industry is therefore crucial in the implementation of the directive

Apart from OES, NIS Directive is also applicable to digital service providers (DSP). DSPs can be search engines, **cloud** computing services, and online marketplaces (e-commerce sites).

- The directive defines an online search engine 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…and returns links in which information related to the requested content can be found."
- The **Communication on the NIS Directive**, which is intended to help member states implement the NIS Directive, noted there are three main types of cloud service models: Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), and Platform-as-a-Service (PaaS).
- The directive makes clear that online marketplaces may include the processing of transactions, aggregations of data, profiling of users, and application software stores.

The European Commission determines security and notification requirements for DSPs, and member states are not allowed to impose stricter requirements on them. Mandatory DSP requirements include security measures for the network and information systems, including incident handling, business continuity, monitoring, auditing and testing, and compliance with international standards. Throughout the directive, there is an emphasis on EU and international standards.

DSPs must take measures to minimize the impact of incidents and notify the national authority or CSIRT without undue delay for incidents having a substantial impact on service, including any impacts of third-party providers. The national authority or CSIRT has the discretion to inform the public or require the DSP to inform them.

NIS Directive Applicability

Although NIS Directive is a European piece of legislation, it has global implications. For instance, the NIS applies to U.S. companies with operations in member states. This means that U.S. companies may have to implement security requirements, turn over operational data to allow national authorities to assess their compliance, and perform required remediation measures.

In addition, if a DSP has a primary business establishment in one member state and networks and systems located in other member states, then the DSP should register with the national authority of its main location, and the national authorities of other member states will cooperate with that national authority. If a company is not established in the EU but offers services within it, the DSP must designate a representative in the EU where its services are offered.

Compliance with the NIS Security Requirements

Meeting the objectives and the security requirements of the NIS Directive can be a tenuous exercise. Information security audits and self–assessment/management exercises are the two major enablers to achieve this objective. The compliance assessment performed by national competent authorities (NCA) is mentioned in articles 14, 15 and 16 of the NIS Directive and defines risk assessment and auditing obligations for the OES and DSP respectively.

- **Article 14:** "Member States shall ensure that operators of essential services take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed."
- **Article 15:** "Member States shall ensure that the competent authorities have the powers and means to require operators of essential services to provide (b) evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor and, in the latter case, to make the results thereof, including the underlying evidence, available to the competent authority."
- **Article 16:** "Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements: a) the security of systems and facilities, b) incident handling, c) business continuity management, d) monitoring, auditing and testing, and e) compliance with international standards."

The EU Cybersecurity Agency (ENISA) has published "Guidelines on assessing DSP security and OES compliance with the NISD security requirements," whose recommendations collectively aim to facilitate NCA conducting audits and to assist DSP and OES across all EU member states to comply with the requirements of the NIS Directive in the effort to achieve a baseline security level.

The ENISA guidelines outline audit and self-assessment/management frameworks that can be applied:

- By both OES and DSP regarding the NIS Directive's security requirements
- As the baseline for building an information security program to manage risk and reduce vulnerabilities
- To define and prioritize the tasks required to enhance security into IT-security risk-based environments

Apart from the ENISA guidelines, UK's NCSC has published the **Cyber Assessment Framework (CAF)**. The CAF collection consists of a set of 14 cybersecurity and resilience principles, grouped in four major objectives, together with guidance on using and applying the principles, and the Cyber Assessment Framework itself.

The CAF provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organization responsible. It is intended to be used either by the responsible organization itself (self-assessment) or by an independent external entity, possibly a regulator or a suitably qualified organization acting on behalf of a regulator.

The NCSC cybersecurity and resilience principles provide the foundations of the CAF. The 14 principles are written in terms of outcomes, i.e. specification of what needs to be achieved rather than a checklist of what needs to be done. The latest version of the NCSC CAF can be found **here**.

The **NIS Directive** is the first EU horizontal legislation addressing cybersecurity challenges. It is a true game-changer for cybersecurity resilience and cooperation in Europe.

As previously noted, the directive has three main objectives:

- Improving national cybersecurity capabilities
- Building cooperation at EU level
- Promoting a culture of **risk management** and incident reporting among key economic actors, notably operators providing essential services (OES) for the maintenance of economic and societal activities and Digital Service Providers (DSP)

The NIS Directive is the cornerstone of the EU's response to the growing cyber threats and challenges which are accompanying the digitalization of our economic and societal life. This article will examine the obligations of the Operators of Essential Services.

The directive compels member states to classify key entities in various critical infrastructure sectors as "Operators of Essential Services" and to ensure that these enterprises have reached a given level of security in terms of their IT systems while imposing a binding reporting obligation on these entities to report incidents. Secondly, and in addition to ensuring that a well-resourced CSIRT is in place, member states will also be required to designate a National Competent Authority (or NCA) to manage reporting and compliance of the OES entities with the directive.

The rationale is that impacts of security incidents in such services may cause major disruptions to economic activities and to society at large, potentially undermining user confidence and causing major damage to the economy of the Union.

Who Are the Operators of Essential Services?

The NIS Directive does not define explicitly which entities are to be considered as OES under its scope. Instead, it provides criteria that member states need to apply in order to carry out an identification process to determine which enterprises will be considered

Sector	Subsector	Type of Entity
Energy	Electricity	Electricity undertakings which carry out the function of "supply"
	Oil	Operators of transmission pipelines
		Operators of oil production, refining, and treatment facilities, storage and transmission
	Gas	Supply undertakings
		Distribution, transmission, and storage system operators
		LNG system operators
		Natural gas undertakings
		Operators of natural gas refining and treatment facilities
Transport	Air transport	Air carriers
		Airport managing bodies, airports, and entities operating ancillary installations within airports
		Traffic management control operators providing air traffic control (ATC) services
	Rail transport	Infrastructure managers
		Railway undertakings
	Water transport	Inland, sea and coastal passenger and freight water transport companies
		Managing bodies of ports including their port facilities
		Operators of vessel traffic services
	Road transport	Road authorities responsible for traffic management control
		Operators of Intelligent Transport Systems
Banking		Credit institutions
Financial market		Operators of trading venues and central counterparties
Health sector	Healthcare settings including hospitals and private clinics	Healthcare providers
Drinking water supply and distribution		Suppliers and distributors of water intended for human consumption
Digital infrastructure		Internet Exchange Points (IXPs)
		DNS service providers
		Top-Level Domain (TLD) name registries

Table 1: Sectors and subsectors subject to the provisions of the NIS Directive.

operators of essential services and therefore subject to the obligations under the directive.

According to Article 5(2), the criteria for the identification of the operators of essential services are the following:

- The entity provides 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
- An incident would have significant disruptive effects on the provision of that service

Article 4(4) of the directive states that an OES is a "public or private entity of a type referred to in Annex II" that meets above criteria. The sectors and subsectors subject to the provisions of the directive are included in Table 1.

While most of the entities belong to "traditional" critical infrastructure sectors, for the digital infrastructure sector, the European Commission **provides further clarifications** to help the member states identify the organizations that fall under this category.

In addition to the above critical sectors, the European Commission **has directed** member states "to expand the security and notification obligations under Article 14 to entities belonging to other sectors and sub-sectors" such as public administrations, food sector, postal sector, chemical and nuclear industry, environmental sector, and civil protection.

Security Requirements for the OES

The NIS Directive requires that member states ensure designated operators of essential services:

- Take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems in the provision of their service [Article 14(1)].
- Take appropriate measures to prevent and minimize the impact of the incidents affecting the security of the network and information systems used in the provision of their service [Article 14(2)].

To help member states develop a harmonized security policy for their OES, the NIS Cooperation Group has published reference security guidelines.

According to the agreed principles, the security measures must be:

- Effective
- Tailored
- Compatible
- Proportionate
- Concrete
- Verifiable
- Inclusive

In addition to the above principles, the NIS Cooperation Group urges member states to "acknowledge the added-value of dialogue with public and private operators, in particular with regard to the implementation of the security measures" and to "find a proper cost-benefit balance so that to ensure efficient security measures, with respect to the security of essential services to the economy and the society, while taking into account their cost for OES."

Based on the Cooperation Group guidelines, each National Competent Authority has published a set of security requirements that OES must implement within their organization. It is the responsibility of the OES to be able to demonstrate to the National Competent Authority that they are applying the mandatory security principles and measures associated with those principles that allow for the protection of network and information security within their organization. OES is responsible for identifying the network and information systems that need to comply with the directive's security requirements, which are to be agreed with the National Competent Authority.

The technical and organizational measures identified in the NIS Cooperation Group guidelines offer a best practice framework for ensuring the protection of network and information systems. The security guidelines consist of five themes that provide a high-level view of an organization's management of cybersecurity risk. These five functions are Identify, Protect, Detect, Respond and Recover, which are in line with the themes of the **NIST** Cybersecurity Framework.

The use of internationally accepted standards and specifications relevant to the security of network and information systems is encouraged in order to promote primary implementations of the requirements. In fact, Ireland's National Cyber Security Center (NCSC) has **published compliance** guidelines that provide a mapping with already established critical infrastructure security frameworks such as CIS Controls, ISA/IEC 62443 standards, ISO 27001:2013 and NIST SP 800-53.

Incident Notification Requirements

According to Article 14(3), member states must ensure that OES notify without any delay "any incident having a significant impact on the continuity of the essential services." Hence, the OESs should only notify serious incidents affecting the continuity of the essential service.

Article 4(7) defines an incident as "any event having an actual adverse effect on the security of network and information systems." The term 'security of network and information systems' is further defined under Article 4(2) as "the ability of network to resists, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems."

Further Guidance

Enterprises that are digital service providers and fall under the provisions of the NIS Directive can seek guidance from either their National Competent Authority or by visiting the **NIS Cooperation Group** website, which has published guidelines to help DSPs **identify cybersecurity incidents** and on **how to notify** such incidents.

Consequently, any event having an adverse effect not only on the availability but also on authenticity, integrity or confidentiality of data or related services could trigger the notification obligation. In fact, the continuity of the service can be compromised not only in cases where the physical availability is concerned but also by any other security incident affecting the proper provision of the service.

In order to determine the significance of the impact of an incident, Article 14(4) states that the following parameters shall be considered:

- The number of users affected by the disruption of the essential service
- The duration of the incident
- The geographical spread regarding the area affected by the incident

Finally, the NIS Cooperation Group has published a **reference document of circumstances** that trigger the notification obligations.

According to these guidelines, the member states can also consider the following parameters to initiate the notification process:

- The dependency of other OES sectors on the service provided by the affected entity
- The impact that incidents have, in terms of degree and duration, on economic and societal activities or public safety
- The market share of that entity
- The importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service

Who are Digital Service Providers (DSPs)?

A "digital service" is defined within the directive (EU) 2015/1535 as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".

For the scope of the NIS Directive, DSPs are limited to only three types of services, as defined in Annex III of the Directive:

- **Cloud** computing service
- Online marketplace
- Online search engines

The directive does not require member states to identify which digital service providers are subject to the relevant obligations. Therefore, the directive's obligations, i.e. the security and notifications requirements set out in Article 16, **apply to all DSPs** within its scope.

Cloud Computing Services

Article 4(19) of the NIS Directive defines cloud computing service as "a digital service that enables access to a scalable and elastic pool of shareable computing resources." The NIS definition has a close alignment with that of **NIST** Special Publication 800-145:

Recital 17 of the directive provides further clarification:

- Cloud computing resources include infrastructure, applications and services accessible in the cloud
- The term "scalable" refers to the flexibility of the cloud computing resources to accommodate fluctuations in workload irrespective of the geographical location of the resources
- The term "elastic pool" is used to describe the availability and the provisioning of the cloud computing resources according to the fluctuations of the workloads
- The term "shareable" is used to describe the ability to provide access to the same cloud computing resources to multiple users

The European Commission further clarified the types of cloud computing services subject to the NIS Directive. These are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a service (SaaS).

However, there are also hybrid models as well as other examples of '[something] as a Service.' If these models meet the definition of "cloud computing service," then NIS also applies to them. The key is whether the service "enables access to a scalable and elastic pool of shareable computing resources."

As detailed in NIST SP 500-292 on Cloud Computing Reference Architecture, the following entities may, depending on the circumstances, enable access to these resources and can be subject to NIS Directive:

- **Cloud provider**—An entity responsible for making a service available to cloud customers because they build and manage cloud infrastructure
- **Cloud broker**—An entity that manages the use, performance and delivery of cloud services, negotiating relationships between cloud providers and cloud customers

Online Market Places

Article 4(17) of the NIS Directive defines online marketplaces as services that "allow consumers and traders to conclude online sales or service contracts with traders and is the final destination for the conclusion of those contracts."

Recital 15 further clarifies that the online marketplace does not cover online services that either serve "only as an intermediary" or "compare the price of particular products or services

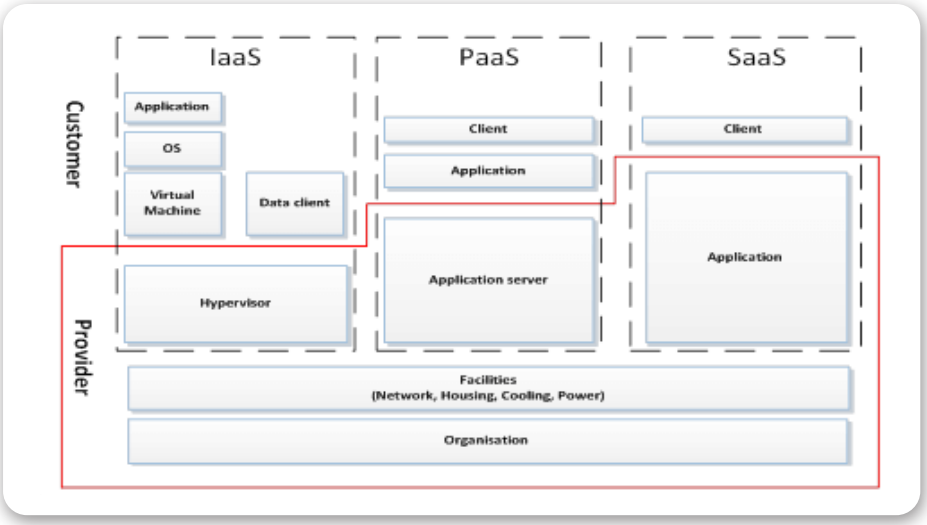

Fig. 1: Types of cloud computing services subject to the NIS Directive.

from different traders" and then redirect the user to the original vendor as Skyscanner does, for example.

The European Commission **further clarified** that computing services provided by the online marketplace may include processing of transactions, aggregations of data or profiling of users. Application stores, which operate as online stores to digitally distribute applications or software programs from third parties, are also a type of online marketplace. For example, a provider such as eBay can be regarded as an online marketplace, as it allows others to set up shops on its platform in order to make their products and services available online to consumers or businesses.

Online Search Engines

Article 4(18) of the NIS Directive defines an online search engine as a digital service that allows users to perform searches on the basis of a query on any subject and returns links in which information related to the requested content can be found. Recital 16 clarifies that "search functions that are limited to the content of a specific website, irrespective of whether the search function is provided by an external search engine," are not subject to the provisions of the directive.

DSPs Security Responsibilities

Article 16(1) of the NIS Directive declares that member states shall ensure that DSPs identify as well as take appropriate and proportionate security measures to manage the risks posed to the integrity, availability and confidentiality of the services they offer within the Union.

These measures should consider the following elements:

- The security of systems and facilities
- Incident handling
- Business continuity management
- Monitoring, auditing and testing
- Compliance with international standards

In addition, Article 16(2) states that member states shall ensure that DSPs take measures to prevent and minimize the impact of security affecting the provision of services within the Union while ensuring the continuity of those services.

DSP Incident Reporting

The NIS Directive does not give a time frame for incident reporting. Article 16(3) states that DSPs shall "notify the competent authority without undue delay of any incident having a substantial impact on the provision of a service." Notifications shall include information to enable the competent authority to determine the significance of any cross-border impact.

Article 16(4) of the directive lists the following five parameters that must be considered in order to determine whether the impact of an incident is substantial:

- The number of users affected by the incident, especially users relying on the (disrupted) service for the provision of their own services
- The duration of the incident
- The geographical spread regarding the area affected by the incident
- The extent of the disruption of the functioning of the service
- The extent of the impact on economic and societal activities

An incident shall be considered as having a substantial impact where at least one of the following situations has taken place:

- The service provided by a digital service provider was unavailable for more than five million user-hours. The term "user-hour" refers to the number of affected users in the Union for a duration of 60 minutes
- The incident has resulted in a loss of integrity, authenticity or confidentiality of stored, transmitted or processed data or the related services offered by a DSP affecting more than 100,000 users in the EU
- The incident has created a risk to public safety, public security or loss of life
- The incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds €1,000,000

Applicability

It is important to note that NIS Directive applicability extends beyond EU borders. While Article 18(1) states that "the Member State where the DSP has its main head office has jurisdiction over the company," Article 18(2) imposes on a DSP the obligation to designate

a representative in the EU if that DSP "offers services in the EU but is not established in the EU territory." In that case, the member state where the representative is established will have jurisdiction over the company.

In cases where a DSP provides services in a member state but has not designated a representative in the EU, the member state can take actions against the DSP, as the provider is violating its obligations which derive from the directive.

Finally, DSPs that are micro or small enterprises, meaning they employ fewer than 50 persons and have an annual turnover and/or an annual balance sheet total not exceeding €10 million, are excluded from the scope of the security requirements and notification set forth under the directive [Article 16(11)].

According to the NIS Directive, member states should adopt a common set of baseline security requirements to ensure a minimum level of harmonized security measures across EU and enhance the overall level of security of operators providing essential services (OES) and digital service providers (DSP).

Fig. 2: The Information Security Audit lifecycle.

To assist organizations in meeting compliance with the directive, the European Union Agency for Cybersecurity (ENISA) and the UK's National Cyber Security Center (NCSC) have developed assessment frameworks.

ENISA Guidelines on Assessing DSP and OES Compliance

According to the NIS Directive Articles 14, 15 and 16, one of the key objectives is to introduce appropriate security measures for OES as well as for the DSP to achieve a common level of information security within the EU network and information systems.

Information security audits and self–assessment/ management exercises are the two major enablers to achieve this objective.

The main objective of the ENISA guidelines is to facilitate National Competent Authorities (NCA) conducting audits and to assist DSP and OES across all EU member states in complying with the requirements of the NIS Directive in the effort to achieve a baseline security level.

The objective of the guidelines is achieved by:

1. Proposing the information security audit and self-assessment/

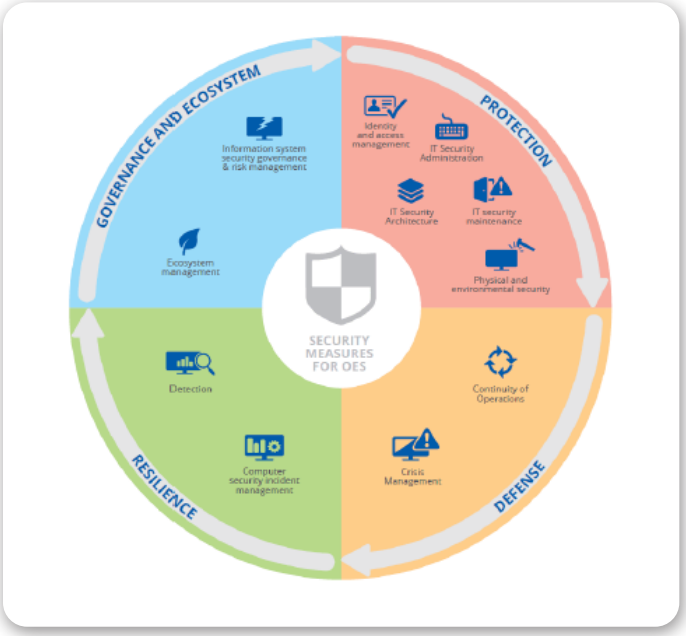

Fig. 3: Security Measures for operators of essential services (OES).

Fig. 4: Security Elements for digital service providers (DSP).

management frameworks that can be applied by DSP and OES with regards to the NIS Directive security requirements

2. Mapping those frameworks per domain of applicability (i.e. in DSP, OES business environments or both)
3. Presenting recommendations to the NCA on how to handle, manage and process the information collected during audits performed on OES

The key outcome of the guidelines is a set of questions and supporting information that NCA can use to assess OES compliance as well as a set of questions for DSP to perform security self-assessments against the NIS security requirements.

The ENISA guidelines present the steps of an information security audit process for the OES compliance as well as of a self-assessment/management framework for the DSP security against the security requirements set by the NIS Directive.

In addition, they provide an analysis of the most relevant information security standards and frameworks, such as **ISO/IEC 27001** and **NIST SP 800-30**, to support OES and DSP in practicing the above exercises in the most tailored and efficient manner. This necessity derives from the fact that there are numerous frameworks developed for specific industries and sectors, incorporating different regulatory compliance goals and varying degrees of complexity and scale. Therefore, the mapping of information security audit and self-assessment/management frameworks for DSP and OES will ensure the cultural coverage of both sectoral and cross sectors (e.g. as energy, transport, drinking water and distribution, banking and financial market infrastructures, healthcare and digital infrastructure) as defined in the ANNEX II of the NIS Directive.

The ENISA guidelines can be applied as the baseline for building an information security program to manage risk and reduce vulnerabilities and to define and prioritize the tasks required to enhance security into IT-security risk-based environments.

Objectives	Description	Sectors
Objective A: Managing security risk	Appropriate organizational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions.	A.1 Governance
		A.2 Risk management
		A.3 Asset management
		A.4 Supply chain
Objective B: Protecting against cyber attack	Proportionate security measures are in place to protect the network and information systems supporting essential functions from cyber-attack.	B.1 Service protection policies and processes
		B.2 Identity and access control
		B.3 Data security
		B.4 System security
		B.5 Resilient networks and systems
		B.6 Staff awareness and training
Objective C: Detecting cyber security events	Capabilities exist to ensure security defenses remain effective and to detect cyber security events affecting, or with the potential to affect, essential functions.	C.1 Security monitoring
		C.2 Proactive security event discovery
Objective D: Minimizing the impact of cyber security incidents	Capabilities exist to minimize the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those functions where necessary.	D.1 Response and recovery planning
		D.2 Lessons learned

Table 1: NCSC Cyber Security and Resilience Principles

Table 2: NCSC Cyber Security and Resilience Principles

	Indicators in CAF IGP are...	Indicators in CAF IGP tables are not...
Purpose	...intended to help inform expert judgement.	...a checklist to be used in an inflexible assessment process.
Scope	...important examples of what an assessor will normally need to consider, which may need to be supplemented in some cases.	... an exhaustive list covering everything an assessor needs to consider.
Applicability	...designed to be widely applicable across different organisations, but applicability needs to be established.	...guaranteed to apply verbatim to all organisations.

Table 3: CAF IGP Tables

NCSC Cyber Assessment Framework

The NCSC **Cyber Assessment Framework (CAF)** provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organization responsible. It is intended to be used either by the responsible organization itself as a self-assessment tool or by an independent external entity, possibly a regulator, like an NCA, or a suitably qualified organization acting on behalf of a regulator.

The CAF collection is aimed at helping an organization achieve and demonstrate an appropriate level of cyber resilience in relation to certain specified essential functions performed by that organization. The NCSC **cyber security and resilience principles** provide the foundations of the CAF. The 14 principles are written in terms of outcomes, i.e. specification of what needs to be achieved rather than a checklist of what needs to be done. The CAF adds additional levels of detail to the top-level principles, including a collection of structured sets of Indicators of Good Practice (IGP).

The CAF has been developed to meet the following set of requirements:

1. Provide a suitable framework to assist in carrying out cyber resilience assessments
2. Maintain the outcome-focused approach of the NCSC cybersecurity and resilience principles and discourage assessments being carried out as tick-box exercises
3. Be compatible with the use of appropriate existing cybersecurity guidance and standards
4. Enable the identification of effective cybersecurity and resilience improvement activities
5. Exist in a common core version which is sector-agnostic
6. Be extensible to accommodate sector-specific elements as may be required
7. Enable the setting of meaningful target security levels for organizations to achieve, possibly reflecting a regulator view of appropriate and proportionate security
8. Be as straightforward and cost-effective to apply as possible

It is important to recognize that the intent is not to produce an all-encompassing cybersecurity "to do" list.

The NCSC intends the principles and guidance to be used in the following way by organizations performing essential functions:

- **Understand the principles and why they are important.** Interpret the principles for the organization
- **Compare the outcomes described in the principles to the organization's current practices.** Use the guidance to inform the comparison
- **Identify shortcomings.** Understand the seriousness of shortcomings using organizational context and prioritize
- **Implement prioritized remediation.** Use the guidance to inform remediation activities

An assessment of the extent to which an organization is meeting a principle is accomplished by assessing all the contributing outcomes for that principle.

In order to inform assessments at the level of contributing outcomes:

- Each contributing outcome is associated with a set of indicators of good practice (IGP)
- Using the relevant IGPs, the circumstances under which the contributing outcome is judged 'achieved,' 'not achieved' or (in some cases) 'partially achieved' are described

For each contributing outcome, the relevant IGPs have been arranged into table format. The resulting tables, referred to as IGP tables, constitute the basic building blocks of the CAF. In this way, each principle is associated with several IGP tables, one table per contributing outcome. The following table summarizes the key points relating to the purpose and nature of the indicators included in the CAF IGP tables.

How Tripwire Can Help

Tripwire can assist organizations meet the NIS Directive objectives and security requirements with a variety of solutions. **Tripwire® Enterprise** is a **security configuration management** solution that allows for real-time detection of threats, anomalies and suspicious changes while providing visibility into the organization's security state. **Tripwire IP360™** is a state-of-the-art, scalable and flexible **vulnerability management** solution that provides meaningful scoring to help improve organizational efficiency and assets visibility. **Tripwire Industrial Visibility and Tripwire Industrial Sentinel** can help organizations map their networks to fix vulnerabilities without interrupting crucial operations while automating **security controls**. Finally, **Tripwire Log Center™** ensures all log data is captured and retained, highlighting critical events and reducing unnecessary noise.

Sources

Table 1: NIS Directive
Tables 2 & 3: NCSC
Fig 1: NIS Directive
Figs 2, 3 & 4: ENISA

About the Author

Anastasios Arampatzis is a retired Hellenic Air Force officer with over 20 years' worth of experience in managing IT projects and evaluating cybersecurity. During his service in the Armed Forces, he was assigned to various key positions in national, NATO and EU headquarters, and has been honored by numerous high-ranking officers for his expertise and professionalism. He was nominated as a certified NATO evaluator for information security.

Anastasios' interests include among others cybersecurity policy and governance, ICS and IoT security, encryption, and certificates management. He is also exploring the human side of cybersecurity—the psychology of security, public education, organizational training programs, and the effect of biases (cultural, heuristic and cognitive) in applying cybersecurity policies and integrating technology into learning. He is intrigued by new challenges, open-minded and flexible.

Currently, he works as a cybersecurity content writer for Bora – IT Security Marketing and is a member of the non-profit organization Homo Digitalis.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

WPNISD1b 2004