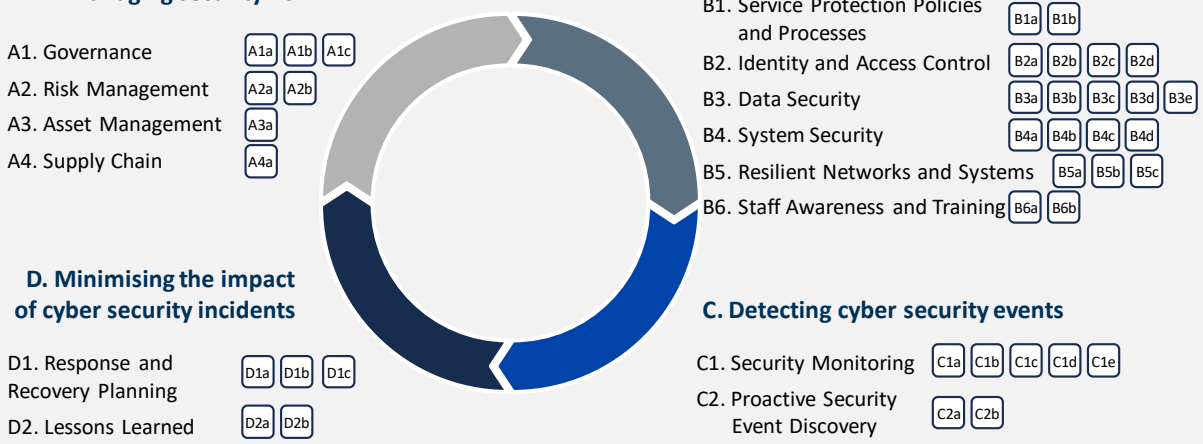
Cetome

Securing a Better Future

November 2019

Author: Dr. Cédric LEVY-BENCHETON, CEO



The NIS Directive is a new regulation, where Operators of Essential Services (OESs) and Digital Service Providers (DSPs) must protect their service against cyber risks. In the UK implementation, the NIS Regulations, the Cyber Assessment Framework (CAF) supports OESs and their Competent Authorities (CAs) in the process of carrying out their regulatory requirements.

This fourth article is part of a series that aims to better apprehend this directive. In this article, we present the UK approach. We introduce the CAF and its IGP tables, and explain how OESs and CAs can use the CAF to assess and improve their security posture on the way to compliance.

The Cyber Assessment Framework is a high-level framework developed by the NCSC that supports OESs and CAs in their compliance with the NIS Regulations. The CAF defines four security objectives:

- **Objective A. Managing security risks**: Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services.
- **Objective B. Protecting against cyber attacks**: Proportionate security measures are in place to protect essential services and systems from cyber-attack
- **Objective C. Detecting cyber security events:** Capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services.
- **Objective D. Minimising the impact of cyber security incidents:** Capabilities to minimise the impact of a cyber security incident on the delivery of essential services including, the restoration of those services, where necessary.

These objectives are interdependent. For instance, it is important to have a strong understand of what to secure (objective A) before protecting it (objective B). Moreover, the CAF contributes to performing continuous security improvement. For example, incidents should contribute to lessons learned and refine existing security measures.

Note: the CAF is used for OESs in every sector under the NIS Regulations except the Health sector, where NHS Digital has developed the DSPT (Data Security and Protection Toolkit). Relevant Digital Service Providers can apply the principles of the CAF.

Each objective is complemented with outcomes and contributing outcomes. In total, there are 14 outcomes and 39 contributing outcomes:

- An **outcome** is a high-level security principle that contributes to attain NIS compliance. For example, "data security" is an outcome of Objective B: it is one element (among others) that contributes to protecting against cyber attacks.

- A **contributing outcome** support the achievement of each security outcome. They present specific requirements to mitigate the cyber risks faced by OESs. For exemple, some contributing outcome for "data security" are "understanding data" and "encryption".

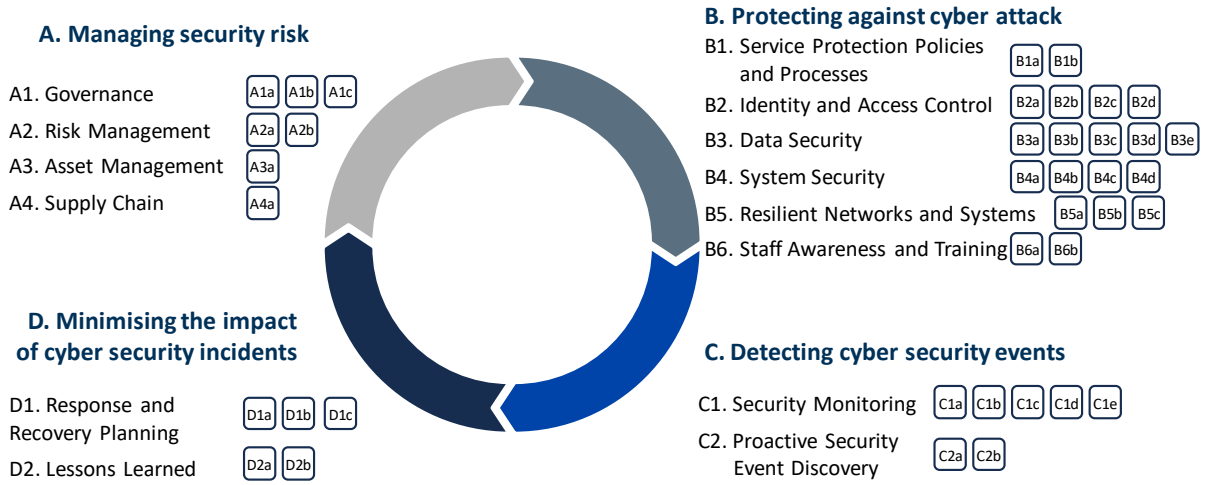


Figure 1. The Cyber Assessment Framework with its 4 objectives, 14 outcomes, and 39 contributing outcomes.

Contributing outcomes can be '**achieved'**, **'not achieved**' or (in some cases) '**partially achieved**'. This means that OESs must assess their security posture and demonstrate they are using appropriate and proportionate security measures in relation to the contributing outcomes.

The NCSC has chosen this approach to discourage assessments being carried out as tick-box exercises. Indeed, it is very common that security compliance is only done "at minimum" to comply with the requirements of a standard. The intent of CAF is to ensure that the cyber risks that may disrupt a service are identified and mitigated. This approach is not too dissimilar from the NIST Cyber Security Framework, with a strong focus on OT security.

Note: It is not expected nor realistic that every contributing outcome is "achieved". CAs expect that OESs understand their gaps and develop appropriate and proportionate security measures to get closer to this status.

The current version of the CAF is sector-agnostic. In the future, the risks could have evolved differently according to the sectors and today's security posture would not be sufficient.

For that purpose, the CAF supports profiles. A CAF profile defines a status for each contributing outcome. It can serve either as an expected baseline or an objective to reach. It is also important that CAF profiles never overlap, so that OESs clearly know what their expectations are!

In the future, when competent authorities have enough information to refine what is expected from OESs in their sector, they can define CAF profiles according to several parameters:

- The level of preparedness of OES in their sector
- The specificities of their OES (size, local/national/cross-border presence, etc.)
- The cyber security risks faced by OES in their sector
- etc.

Note: It makes sense to have sector-specific CAF profiles as the risks apply differently to the various NIS sectors and sub-sectors. These CAF profiles shall also evolve through time to take into account the evolution of each sector, new threats, etc.

The NCSC has developed Indicators of Good Practices (IGPs) to help OESs assess their security. IGPs give an idea of what can be done to achieve a security outcome. These are strictly indicative, and certainly not prescriptive.

The indicators of good practices are presented in tables (IGP Table) that allow to assess the security posture for each contributing outcome (i.e. not achieved, partially achieved or achieved).

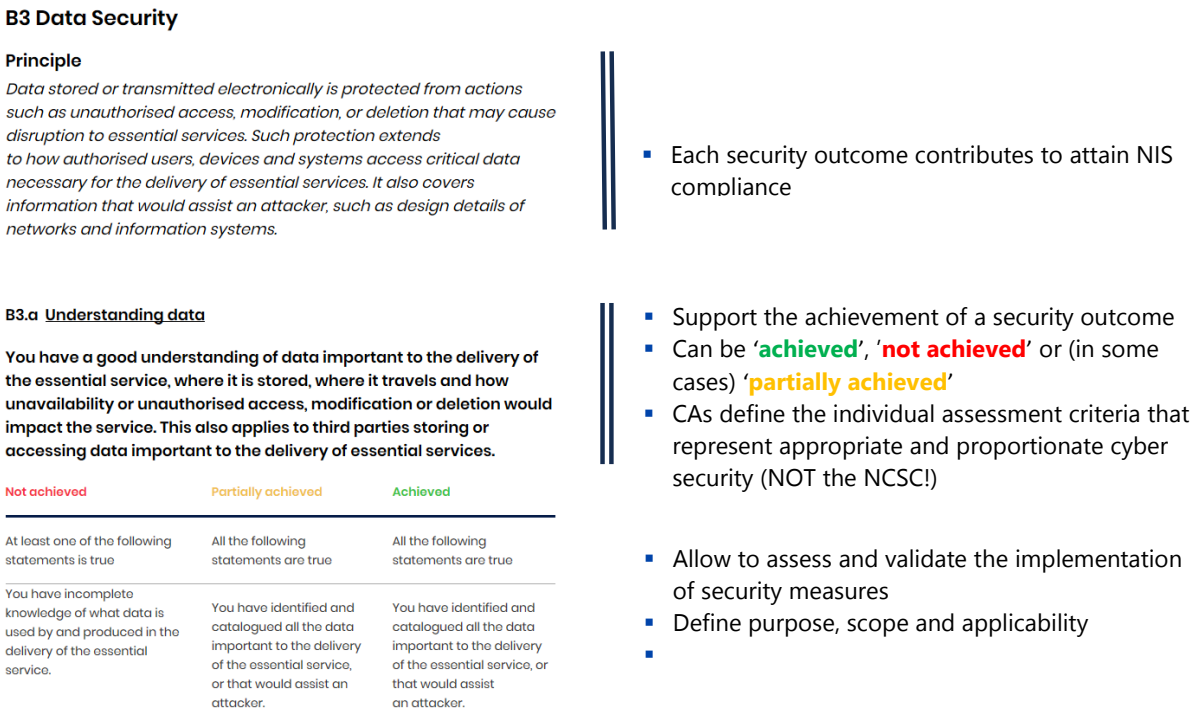


Figure 2. The CAF and IGP tables

As the NCSC explains on its website, the IGP Tables are NOT a checklist! They do not provide an exhaustive list covering everything an assessor needs to consider, and they may not apply verbatim to all organisations.

It is best to see IGP tables as guidance: they give an idea of what is expected to reach an "achieved" status for each contributing outcome. By reading the content of IGP tables, it is clear

that many statements relate to other contributing outcomes: this requires prioritising some contributing outcomes.

Another important thing to consider when using IGP tables is the transition from "not achieved" to "achieved":

- A contributing outcome is "not achieved" when at least one of the states is true.
- Reaching "partially achieved" and "achieved" requires that all statements are true.
- Moving from "partially achieved" to "achieved" usually requires a time-based approach to security, with requirements around security management and continuous improvement.

Note: It is possible for an OES to find itself in a state between "not achieved" and "(partially) achieved". It is not an issue, as OESs must justify their posture to their CA and provide an improvement roadmap.

It is important to understand that the CAF is not "yet another standard". As such, the CAF proposes a mapping of its different objectives with existing standards and guidance. Moreover, the goal of the CAF is to avoid several issues related to compliance-based approaches (all-or-nothing approach, rarely focuses on the content, security efforts can be limited in time, etc.).

The CAF forces OESs to adopt a modern vision around security objectives. It requires security to become a matter at board-level. Moreover, it promotes a flexible approach where security measures depend on the threats and risks faced while adapting to the organisation, its structure and culture. To simplify this matter, the NCSC has mapped several security good practices, guidance, and standards to each contributing outcome.

By being generic enough and with a focus on OT, the CAF is reusable by non-regulated sectors such as manufacturing or the pharmaceutical industry.

Under the NIS Regulations, the CAF is currently used in two ways:

1) OESs use the CAF to fulfil their regulatory requirements. They perform a self-assessment and provide the results to their CA (the "CAF returns") as well as an improvement roadmap. In this case, OESs must assess their security posture against each contributing outcome. They can explain how their security measures are appropriate and proportionate to mitigate the risks they face. For that, they can rely to the IGP tables. They can also explain why they have decided not to implement a specific security measure.

2) Competent Authorities analyse the CAF returns and the improvement roadmap of their OESs. For that, they will assess whether OESs implement appropriate and proportionate security measures according to their self-assessment, their CAF profile, and possible on-site inspections.

Even though the CAF is designed to be flexible, it can be complex. Indeed, several OESs may have different business lines or different geographical sites with their own security measures. However, one organisation must provide one single CAF return to its regulator.

Note: In the energy domain, the regulator gave OESs the possibility to provide a "sub-CAF" for each sub-domains/site/etc. They must also join a main CAF return showing the lowest common denominator for each contributing outcome.

In the UK, the NIS Directive requires OESs to perform a self-assessment of their security posture using the Cyber Assessment Framework (CAF), an outcome-based framework. The CAF proposes a flexible approach to security. It defines 4 security objectives, with 14 outcomes and 39 contributing outcomes that can be "not achieved", "partially achieved" or "achieved".

The CAF is accompanied by Indicators of Good Practice (IGPs) that give an idea of achieving each contributing outcome. However, these IGPs are not a checklist and each OES must assess and justify their security measures. They must also develop an improvement roadmap.

CAs analyse "CAF returns" and improvement roadmap, and ensure that the security measures of their OESs remain appropriate and proportionate. This is currently in progress.

In the future, the CAF will evolve to make it easier to use. Moreover, CAs will have the opportunity to develop their own sector-specific profiles to accompany OESs in their security journey.

Dr. Cédric LÉVY-BENCHETON is the CEO and founder of Cetome. Cédric has expertise in the NIS Directive and OT/ICS security. Cédric previously worked at ENISA, the European Union Cyber Security Agency. Before that, Cédric designed critical networks for public transports.

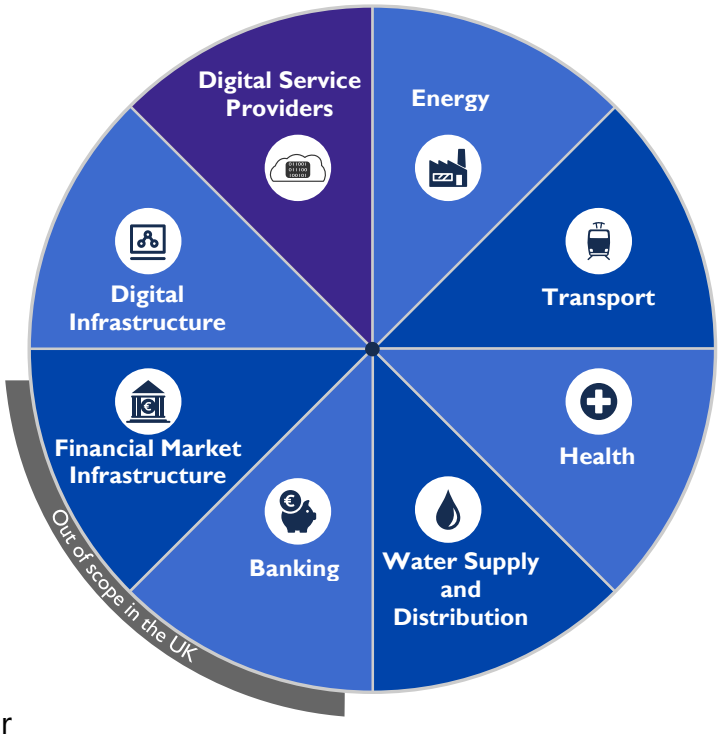
Cetome
Securing a Better Future

The GDPR of Critical Infrastructure

Several recent cyber attacks have disrupted critical national infrastructure with an **impact on our economy and our safety**. For this reason, the European Union and its Member States (including the UK) have voted the **NIS Directive** to better protect our society from cyber risks.

Where does it apply?

The NIS Directive applies to **Operators of Essential Services** which provide a service vital to the society, and to **Digital Service Providers** which operate Cloud services, search engines or online marketplaces.



The sectors in scope

- **Implement**
- **Notify**

without delay.

important penalty

You must comply with the NIS Directive if your organisation meets the criteria established by your Competent Authority.

Objectives of the Directive

- Understand and prevent **cyber risks** by securing network and information systems
- Augment the preparedness and **trust in critical infrastructure** across Europe and the UK
- Ensure the thorough implementation of **good security practices and cyber resilience**
- Handle incidents to **minimise impact on service** and develop lessons-learned

Why Choose Cetome ?

We started Cetome with the desire to help you **do the right thing at the right time!** We make sure that your activity is **secure against cyber risks** in **compliance with the requirements** of the NIS Directive. Our experts have worked at ENISA and have contributed to the NIS Directive.

Our Services

Cetome
Securing a Better Future

If you are an **Operators of Essential Services** or a **Digital Service Provider** in Europe or in the UK, we have developed solutions to help you prepare and comply with the NIS Directive.

Readiness Assessment

We look at your **existing security measures** and **identify improvements** to better protect of your critical service. You receive:

-
-
-

Appropriate Security Measures

We define and implement appropriate and proportionate security measures to **protect you** from cyber risks you face **without disruption**. You receive:

-
-
-

OT Security

We develop appropriate security measures to **protect your OT systems** from cyber attacks. You receive:

-
-
-

e.g.

Compliance Programme

We support your NIS Directive compliance by **accompanying you** in your self-assessment and for **your improvement roadmap**. You receive:

-
-
-

Awareness and Training

We make sure your board and your staff understand their **obligations** and what constitutes a **successful NIS Directive implementation**. You receive:

-
-

Cetome has trained several Competent Authorities and OESs.

Contact Us

Email: _____
Website: _____

Download our white papers on the NIS Directive from our website.