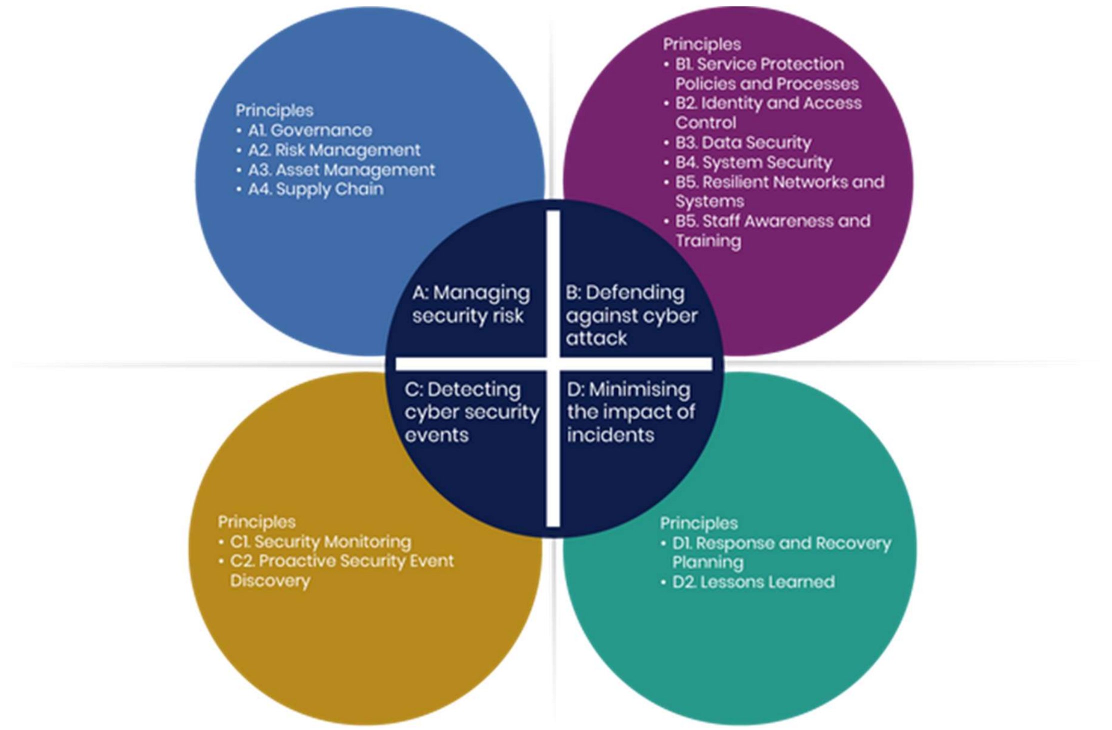
Introduction to the Cyber Assessment Framework


Principles
• A1. Governance
• A2. Risk Management
• A3. Asset Management
• A4. Supply Chain
Principles
• B1. Service Protection Policies and Processes
• B2. Identity and Access Control
• B3. Data Security
• B4. System Security
• B5. Resilient Networks and Systems
• B5. Staff Awareness and Training
A: Managing security risk
B: Defending against cyber attack
C: Detecting cyber security events
D: Minimising the impact of incidents
Principles
• C1. Security Monitoring
• C2. Proactive Security Event Discovery
Principles
• D1. Response and Recovery Planning
• D2. Lessons Learned

On this page:

The CAF – a tool for assessing cyber resilience

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 organisation responsible. CAF-based assessments can be carried out either by the responsible organisation itself (self-assessment) or by an independent external entity, possibly a regulator / cyber oversight body or a suitably qualified organisation acting on behalf of a regulator, such as an NCSC assured commercial service provider.

The NCSC CAF cyber security and resilience objectives and principles provide the foundations of the CAF. The 4 high-level objectives (A-D) and the 14 principles laid out within this collection 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 (IGPs).

Note

The NCSC developed the CAF in its role as national technical authority for cyber security with an expectation that it would be used, amongst other things, as a tool to support effective cyber regulation. The NCSC itself has no regulatory responsibilities, and organisations subject to cyber regulation should consult with their regulators to learn whether they should use the CAF in the context of meeting regulatory requirements.

CAF requirements

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

1. **1**

provide a suitable framework to assist in carrying out cyber resilience assessments

2. **2**

maintain the outcome-focused approach of the NCSC cyber security and resilience principles and discourage assessments being carried out as tick-box exercises

3. **3**

be compatible with the use of appropriate existing cyber security guidance and standards

4. **4**

enable the identification of effective cyber security and resilience improvement activities

5. **5**

exist in a common core version which is sector-agnostic

6. **6**

be extensible to accommodate sector-specific elements as may be required

7. **7**

enable the setting of meaningful target security levels for organisations to achieve, possibly reflecting a regulator view of appropriate and proportionate security

8. **8**

be as straightforward and cost-effective to apply as possible

---

How the CAF collection is intended to be used - an outcome-based approach

The NCSC is committed to working constructively with regulators, Lead Government Departments for CNI sectors, industry and other stakeholders to help ensure that the most nationally important networks and information systems are subject to effective cyber risk management regimes. This commitment has shaped the NCSC approach to developing the CAF collection.

When considering approaches to driving change toward a recognised desirable end-state, two fundamental methods exist:

1. **1**

Prescriptive Rules Approach:

- In this method, a specific set of **detailed rules** is established. These rules prescribe precisely what actions are permissible and what constitutes undesirable conduct.
- When followed closely, these rules can lead to achieving the desired end-state.
- However, there’s a catch: prescriptive rules must account for **all possible scenarios**, which can be challenging in complex and rapidly evolving domains.
- Attempting to create exhaustive rules, especially in areas like **cyber security**, often results in **unintended consequences**, misallocation of resources, and limited benefits.

2. **2**

Principles-Based Approach:

- Instead of rigid rules, this approach relies on a **set of principles** to guide decision-making.
- These principles serve as general guidelines, allowing flexibility in adapting to diverse situations.

- The **NCSC** advocates for this approach, emphasising its effectiveness in driving improvements to cyber security and resilience.
- Principles align with the majority of **goal-based regulations** in the UK, emphasising outcomes over rigid prescriptions.

In summary, while prescriptive rules have their place, the principles-based approach offers adaptability and resilience, especially in dynamic fields like cyber security. This is why the NCSC has developed such a set of principles as part of the CAF collection.

The CAF principles define a set of top-level outcomes that, collectively, describes good cyber security and resilience for organisations performing essential functions. Each principle is accompanied by a narrative which provides more detail, including why the principle is important. Additionally, each principle is supported by a collection of relevant guidance which both highlights some of the relevant factors that an organisation will usually need to take into account when deciding how to achieve the outcome, and recommends some ways to tackle common cyber security challenges.

Some organisations may be concerned that the principles and guidance are too vague. It is important to recognise that the intent is not to produce an all-encompassing cyber security and resilience *"to do"* list – an unachievable goal in any case. Organisations understand their own business better than any external entity, and should be capable of taking informed, balanced decisions about how they achieve the outcomes specified by the principles. The NCSC intends the principles and guidance to be used in the following way by organisations performing essential functions:

1.

Understand the principles and why they are important.

2.

Interpret the principles for the organisation.

3.

Compare the outcomes described in the principles to the organisation's current practices using the guidance.

4.

Identify shortcomings and understand the seriousness of shortcomings using organisational context and prioritise them.

5.

Implement remediation by addressing prioritised issues using the guidance.

CAF principles and contributing outcomes

Each top-level NCSC security and resilience principle defines a reasonably wide-ranging outcome. The precise approach organisations should adopt to achieve each principle is not specified as this will vary according to organisational circumstances. However, each principle can be broken down into a collection of lower-level **contributing** [cyber security and resilience] **outcomes**, all of which will normally need to be achieved to fully satisfy the top-level principle.

An assessment of the extent to which an organisation is meeting a particular principle is accomplished by assessing all the contributing outcomes for that principle. In order to inform assessments at the level of contributing outcomes:

1. **1**

each contributing outcome is associated with a set of indicators of good practice (IGPs) and,

2. **2**

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 conveniently 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 tables of IGPs, one table per contributing outcome.

Using IGPs

Assessment of contributing outcomes is primarily a matter of **expert judgement** and the IGPs do not remove the requirement for the informed use of cyber security expertise and sector knowledge. IGPs will usually provide good starting points for assessments but should be used flexibly and in conjunction with the NCSC guidance associated with the top-level cyber security and resilience principles. Conclusions about an organisation’s cyber security and resilience should only be drawn after considering additional relevant factors and special circumstances.

The ‘achieved’ (GREEN) column of an IGP table defines the typical characteristics of an organisation fully achieving that outcome. It is intended that all the indicators would normally be present to support an assessment of ‘achieved’. The exception would be when an IGP may not be applicable if there are compensating measures that would meet the requirements of the relevant objective.

The ‘not achieved’ (RED) column of an IGP table defines the typical characteristics of an organisation not achieving that outcome. It is intended that the presence of any one indicator would normally be sufficient to justify an assessment of ‘not achieved’.

When present, the ‘partially achieved’ (AMBER) column of an IGP table defines the typical characteristics of an organisation partially achieving that outcome. It is also important that the partial achievement is delivering specific worthwhile cyber security and resilience benefits. An assessment of ‘partially achieved’ should represent more than giving credit for doing something vaguely relevant.

The following table summarises the key points relating to the purpose and nature of IGPs:

Setting target levels of cyber security and resilience

The result of applying the CAF is 39 individual assessments, each one derived from making a judgement on the extent to which a set of IGPs reflects the circumstances of the organisation being assessed. The CAF has been designed in such a way that a result in which all 39 contributing outcomes were assessed as ‘achieved’ would indicate a level of cyber security some way beyond the bare minimum ‘basic cyber hygiene’ level.

A cyber oversight body will need to set target levels of cyber resilience for organisations within their sector. One way of setting these target levels is in relation to the *ability to withstand specified categories of cyber attacks* (e.g. resilience to basic capability attacks, moderate capability attacks etc.) and the CAF has been designed to support this approach via the idea of **CAF profiles.**

The NCSC has worked with regulators and other organisations with a cyber resilience oversight role on an approach to interpreting CAF output based on identifying those contributing outcomes considered most important to achieve in order to manage security risks to that organisation’s essential functions. Those prioritised contributing outcomes would correspond to an initial view of appropriate and proportionate cyber security for that organisation. The subset of contributing outcomes identified as the most important in this way would represent an example of a CAF profile – something that could be used as the basis for setting a target for organisations to achieve.

In practice a CAF profile consists of a mixture of some contributing outcomes to be met at ‘achieved’, some at ‘partially achieved’ and perhaps some (representing cyber security capabilities not appropriate at the level of the profile) identified as ‘not applicable’.

It is not the responsibility of the NCSC to mandate what represents appropriate and proportionate (as defined in the NIS Regulations) cyber security and resilience. Any target set for organisations to achieve in terms of CAF results is for the relevant cyber oversight body to define.

Making the CAF sector specific

The common core of the CAF (consisting of principles, contributing outcomes and indicators of good practice) is sector agnostic in the sense that it is designed to be generally applicable to all organisations responsible for essential functions across all key sectors. It is possible that there will be a need for some sector specific aspects of the CAF, which could include the following:

1. **1**

Sector-specific CAF profiles

Some target profiles may well be sector specific. As mentioned in the section on setting target levels, it will be a decision for the relevant cyber oversight body to put an interpretation on CAF results, which may be from a regulatory perspective.

2. **2**

Sector-specific interpretations of contributing outcomes/IGPs

It may be necessary in some cases for a sector-specific interpretation of contributing outcomes and/or IGPs to better clarify meaning within the sector.

3. 3

Sector-specific additional contributing outcomes/IGPs

There may be circumstances in which sector-specific cyber security requirements cannot be adequately covered by an interpretation of a generic contributing outcome or IGP. In these cases, an additional sector-specific contributing outcome or IGP may need to be defined.

The NCSC will continue to work with the full range of CAF stakeholders to determine if sector-specific aspects of the CAF are required, and to assist in considering and introducing changes as necessary.

Cyber Resilience Audit Scheme

To support the use of the CAF, we recommend the use of NCSC's Cyber Resilience Audit (CRA) scheme where appropriate. The CRA scheme provides a list of assured commercial suppliers that can deliver independent CAF-based cyber resilience audits for customers in a range of sectors. An independent audit is likely to be more reliable than a self-assessment, providing a more accurate picture of organisational cyber resilience and informing better cyber resilience assessments at the sector and national levels.

The NCSC is the CRA scheme owner, working closely with any cyber oversight bodies (such as cyber regulators) that choose to use the scheme as scheme partners. The scheme has been built with flexibility in mind, allowing Scheme Partners the ability to define their own sector-specific requirements, assurance, and documentation to act as a sector-specific implementation of the CRA scheme.