Understanding and addressing cyber risks with GovAssure

A BSI white paper

1. Introduction

In 2020, ransomware attacks affecting Redcar & Cleveland and Hackney councils highlighted the severe impact of cybersecurity attacks on critical public services. Unfortunately, this type of attack has become more common; of the 777 cybersecurity incidents managed by the NCSC between September 2020 and August 2021, around 40% were aimed at the public sector. In order to understand and address the cyber risks to the public sector, the GovAssure assessment scheme has been developed and must be performed by all government bodies between now and 2030. GovAssure replaces the cyber security element of the Departmental Security Health Check (DSHC) and is designed for OFFICIAL data.

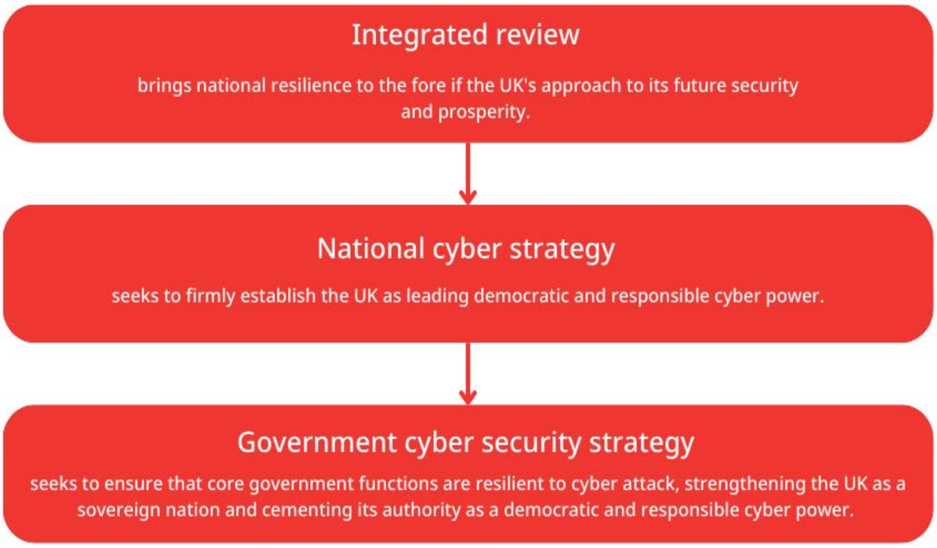
2. The Government Cyber Security Strategy (GCSS)

Through the Integrated Review and National Cyber Strategy, the UK government has outlined its ambition to 'firmly establish the UK as a democratic and responsible cyber power, able to protect and promote its interests as a sovereign nation in a world fundamentally shaped by technology.'

Developing cyber resilience within UK government and public sector organisations is a key part of this ambition. This is underpinned by The Government Cyber Security Strategy: 2022 to 2030 (GCSS), which aims for critical government functions to be significantly hardened to cyberattacks by 2025, with all government organisations across the public sector being resilient to known vulnerabilities and attack methods by 2030.

Figure 1 below shows the relationship between the Integrated Review, National Cyber Strategy, and GCSS.

Figure 1 Strategic Context



Integrated review

brings national resilience to the fore if the UK's approach to its future security and prosperity.

National cyber strategy

seeks to firmly establish the UK as leading democratic and responsible cyber power.

Government cyber security strategy

seeks to ensure that core government functions are resilient to cyber attack, strengthening the UK as a sovereign nation and cementing its authority as a democratic and responsible cyber power.

Strategic Pillars

The GCSS sets out two strategic pillars.

Build organisational cyber resilience

Defend as one

Pillar 1: Build organisational cyber resilience

- Pillar 1 aims to ensure that government organisations have the right structures, mechanisms, tools and support in place to manage their cybersecurity risks.

Pillar 2: Defend as one

- Pillar 2 seeks to harness the value of sharing cybersecurity data, expertise and capabilities across government to present a defensive force disproportionately more powerful than the sum of its parts.

3. GovAssure

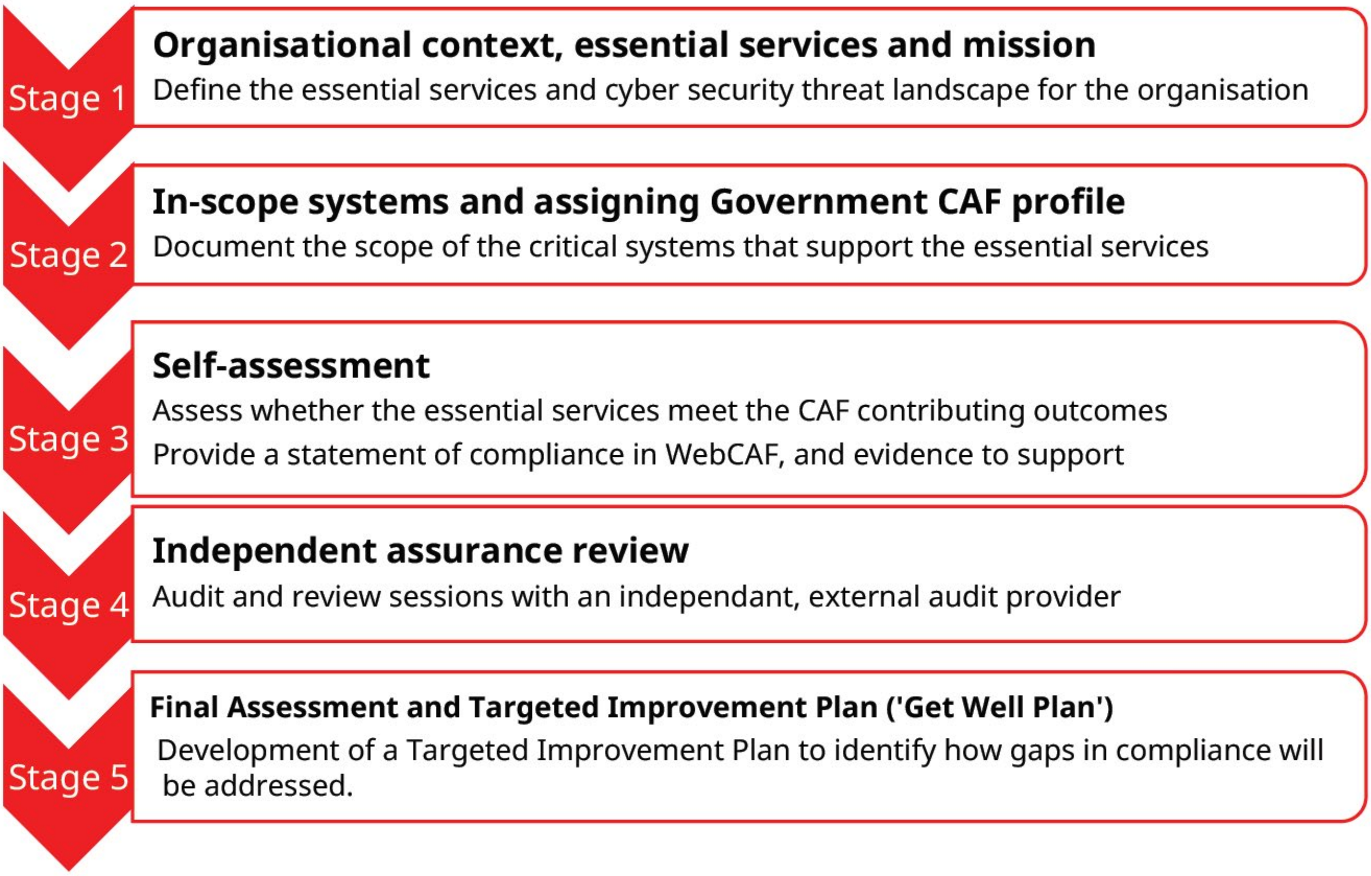
The GovAssure scheme is designed to support the GCSS aims by using the NCSC Cyber Assessment Framework (CAF) to define good practice and measure government and national infrastructure organisations against that good practice. The adoption of the CAF provides a common framework to understand and manage cybersecurity risks more efficiently.

The GovAssure scheme requires that organisations review each of the CAF indicators of good practice (IGPs), and state whether they meet the requirement. Each IGP must also have a justification for the response, and evidence of the activities being implemented in practice.

The responses are then validated by a third party to ensure responses are consistent across departments, and to enable a collaborative and standardised approach. Departments must also plan activities to close any gaps between the required level of compliance and the actual responses documented.

GovAssure stages

GovAssure is broken down into five stages :



Stage 1

Organisational context, essential services and mission

Define the essential services and cyber security threat landscape for the organisation

Stage 2

In-scope systems and assigning Government CAF profile

Document the scope of the critical systems that support the essential services

Stage 3

Self-assessment

Assess whether the essential services meet the CAF contributing outcomes

Provide a statement of compliance in WebCAF, and evidence to support

Stage 4

Independent assurance review

Audit and review sessions with an independant, external audit provider

Stage 5

Final Assessment and Targeted Improvement Plan ('Get Well Plan')

Development of a Targeted Improvement Plan to identify how gaps in compliance will be addressed.

Timeline

Each area of government has been given a target date for compliance, between 2025 and 2030, which is proportionate to the level of risk.

- Government organisations responsible for critical functions will meet the outcomes set out in an 'enhanced' CAF profile by 2025.
- All central government departments will meet outcomes set out in their designated CAF profiles by 2026.
- All other government organisations will meet outcomes set out in a 'basic' CAF profile by 2030.

Baseline vs enhanced profile

Organisations do not need to achieve all the IGPs, but need to comply with either the baseline or enhanced profiles, developed by The Government Security Group (GSG), the NCSC and other government bodies.

The baseline profile was developed by modelling the most likely impactful attacks against government and determining the indicators of good practice within the outcomes of the CAF which would mitigate the attack. The same approach was taken to develop the enhanced profile, however, additional higher threat attack scenarios were modelled in the process.

Glossary

Term	Meaning
NCSC - National Cyber Security Center	The national body which defines the CAF
IGP - Indicator of good practice	The detailed list of requirements that define the Outcomes needed for GovAssure
CAF - Cyber Assessment Framework	The set of Objectives, Principles and Outcomes that define the requirements for GovAssure
WebCAF	An online portal for organisations to upload their responses to each IGP.
GCSS - Government Cyber Security Strategy	The overarching plan for UK Government cybersecurity that has led to GovAssure

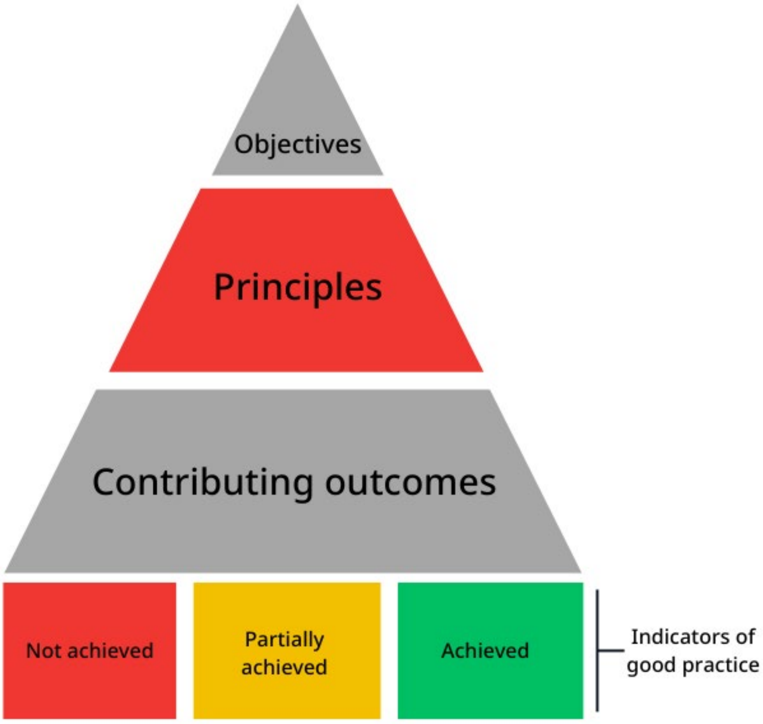
4. GovAssure and the NCSC CAF

CAF overview

The Cyber Assessment Framework (CAF) came out of the EU Network and Information Systems (NIS) Regulations which required organisations to regularly assess their security. In response, The NCSC created the CAF which is a structured, outcome-based way of looking at a system's security and determining its compliance against a range of security subject areas.

There are four overarching objectives, split into 14 principles which are written in terms of 'outcomes', i.e. specifying what needs to be achieved, rather than a checklist of what needs to be done. The CAF adds extra levels of detail to the top-level principles, including a collection of structured sets of IGPs.

The approach organisations adopt to achieve each principle will vary according to the organisational circumstances. However, each principle can be broken down into a collection of lower level contributing cybersecurity and resilience outcomes. The lower-level outcomes must be achieved to fully satisfy the top-level principles and objectives.



Objectives

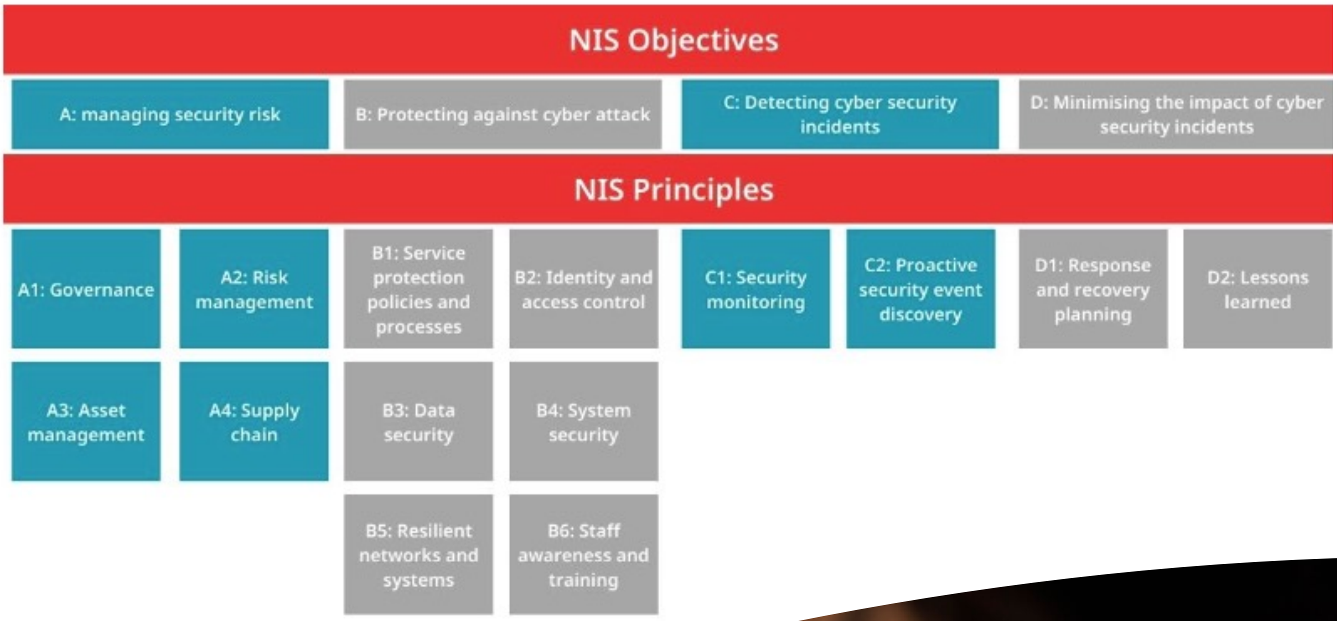
The four interdependent security objectives are:

- **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 cyberattacks:** Proportionate security measures are in place to protect essential services and systems from cyber-attack
- **Objective C. Detecting cybersecurity events:** Capabilities to ensure security defences remain effective and to detect cybersecurity 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 cybersecurity incident on the delivery of essential services including, the restoration of those services, where necessary.

Principles and Contributing outcomes

Each of the four objectives splits into a number of principles and is complemented with contributing outcomes. In total, there are 14 principles split into 39 contributing outcomes, and each principle contains at least one contributing outcome.

A 'contributing outcome' supports the achievement of each principle. They present specific requirements to treat the cyber risks faced by organisations. For example, Objective B (Protecting against cyberattacks) has 6 Principles, including Data Security (Principle B3). Data Security (B3) has 5 Contributing Outcomes, and each of those has a series of IGPs.



NIS Objectives

A: managing security risk

B: Protecting against cyber attack

C: Detecting cyber security incidents

D: Minimising the impact of cyber security incidents

NIS Principles

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 networks and systems

B6: Staff awareness and training

C1: Security monitoring

C2: Proactive security event discovery

D1: Response and recovery planning

D2: Lessons learned

Indicators of Good Practices (IGP)

The NCSC has developed IGPsto help organisations assess their security. IGPs give an idea of how to achieve a security outcome. Using the relevant IGPs, the circumstances under which the contributing outcome is judged 'achieved', 'not achieved' or (in some cases) 'partially achieved' are described.

The IGPs are presented in tables that allow organisations to assess the security posture for each contributing outcome (i.e. not achieved, partially achieved or achieved).

In order to attain an 'achieved' result, an organisation;

- Must answer 'Yes or 'NA' to all Achieved IGPs
- Must answer 'Yes or 'NA' to all Partially Achieved IGPs
- Must answer 'No' or 'NA' to all Not Achieved IGPs

In order to attain a 'partially achieved' result, an organisation;

- Can answer 'No' to some or all of the Achieved IGPs
- Must answer 'Yes or 'NA' to all Partially Achieved IGPs
- Must answer 'No' or 'NA' to all Not Achieved IGPs

Self-assessment and evidence

The organisation must complete a self-assessment, by reviewing the requirements against each critical system to decide whether they have achieved the IGPs or not. In addition, a descriptive statement is provided to define how they meet the IGP, and what evidence can be provided to verify the statements.

Self-assessments can be challenging to complete consistently, as each responder may have their own interpretation and perspective. Therefore, it is useful to produce guidelines, and support for internal staff completing the work. In addition, it is important to collect the evidence of compliance so that when asked later, responses can be supported and justified. This helps to keep responses consistent, and produce practical and proportionate actions to close gaps.

Once the self-assessment has been completed, organisations can choose how to proceed and which gaps should be prioritised, based on the CAF Level (baseline or enhanced), and the specific gaps identified.
It is also important to understand that not every organisation will score 'achieved' for each contributing outcome across each system. Targets will be driven through the assignment of a target CAF profile (baseline or enhanced) and it is important that individuals are aware of this prior to completing the self-assessment.

WebCAF

The webCAF is a portal where organisations document their compliance level against each IGP and provide a justification for each response. The descriptive justification statement provided by the organisation should be sufficiently detailed to allow the independent reviewer to perform an initial desk-based review, supported by appropriate evidence stored in an organised manner.

From here, the independent assessors can review the responses to verify whether the self-assessed compliance level is accurate. The independent assessors then provide a final report of the assessment against the profile, detailing challenges, and any key observations, particularly around areas of non-compliance.

Individuals submitting a CAF self-assessment through WebCAF are responsible for their organisation's return and should make sure that it is subject to appropriate control checks and sign-offs before submitting. It is important to outline who will be involved as early in the GovAssure process as possible to ensure that you have the resource in place to assist with collecting and collating the evidence.

5. BSI GovAssure services

BSI Digital Trust Consulting can support in several ways.

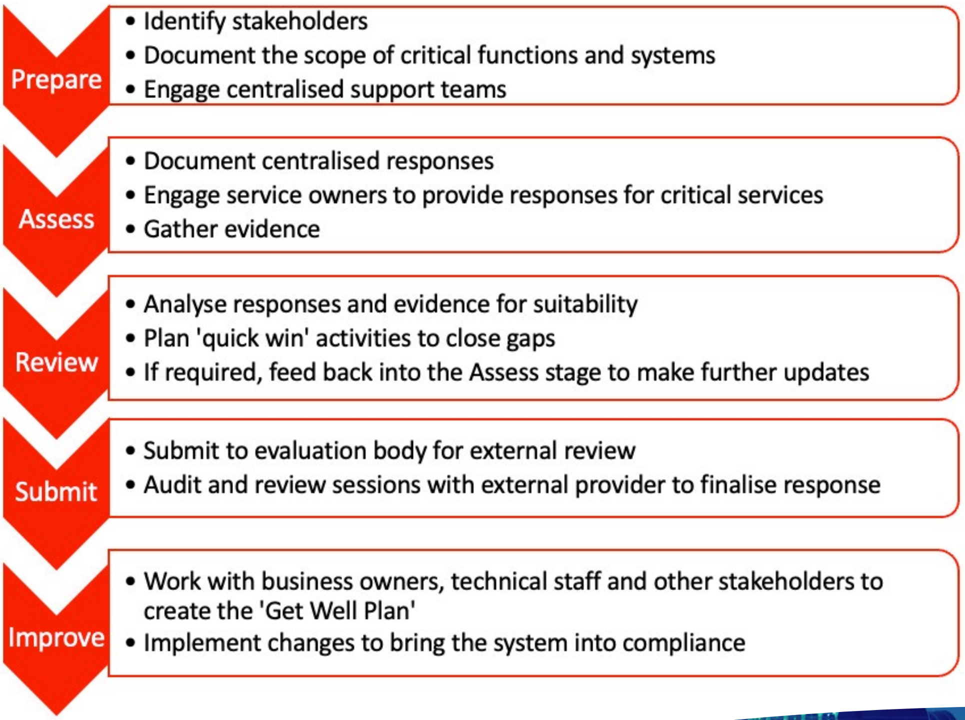
Independent External Assessors

BSI are qualified to perform the role of independent assessor. In this role they can assess and evaluate your compliance to the Baseline or Enhanced profiles. Following the evaluation, we will issue a report.

We are only able to fulfil this role if we have not been involved in the implementation of any of the controls being assessed. We must always maintain our independence and professional integrity.

Planning and supporting the GovAssure scheme

BSI's GovAssure strategy framework can be used to approach the complex task of breaking down the requirements and responses.



Prepare
- Identify stakeholders
- Document the scope of critical functions and systems
- Engage centralised support teams

Assess
- Document centralised responses
- Engage service owners to provide responses for critical services
- Gather evidence

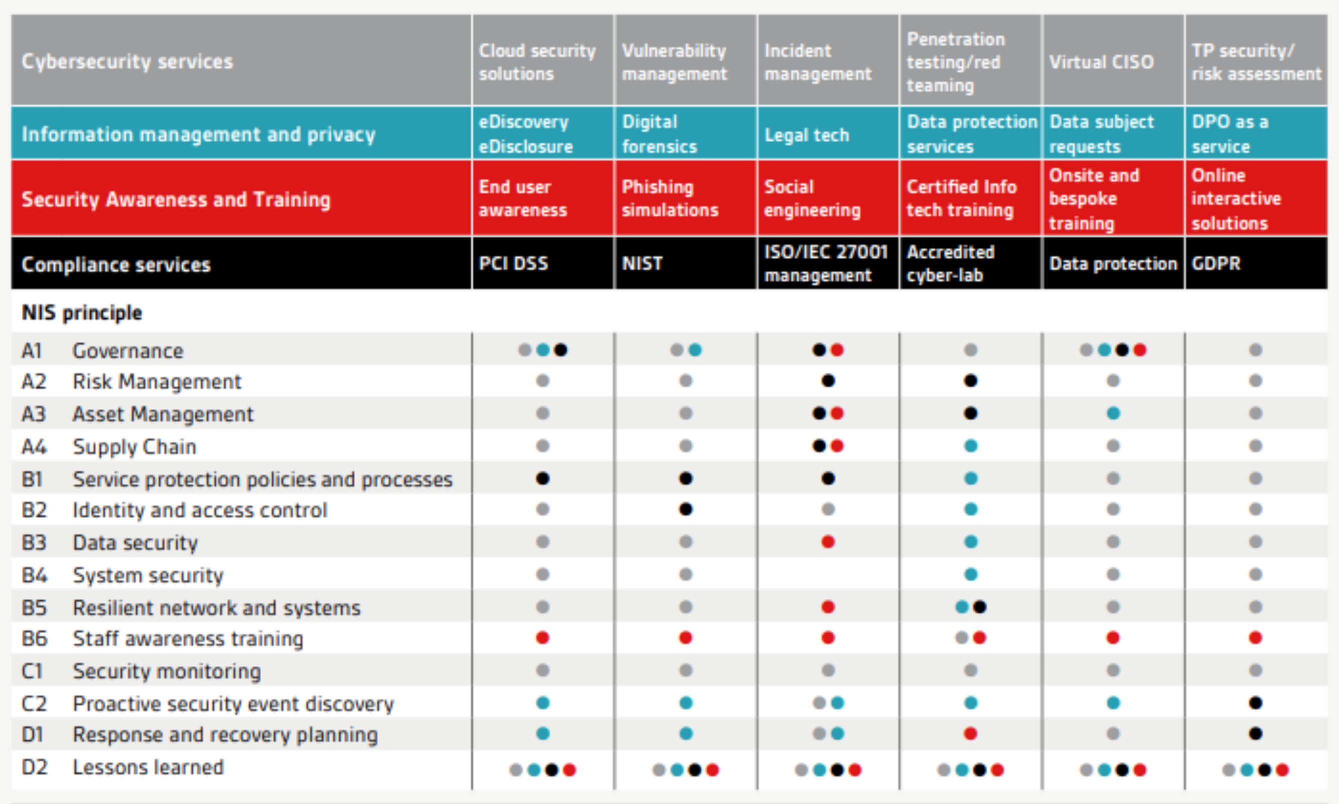
Review
- Analyse responses and evidence for suitability
- Plan 'quick win' activities to close gaps
- If required, feed back into the Assess stage to make further updates

Submit
- Submit to evaluation body for external review
- Audit and review sessions with external provider to finalise response

Improve
- Work with business owners, technical staff and other stakeholders to create the 'Get Well Plan'
- Implement changes to bring the system into compliance

Closing gaps and implementing controls

In addition to managing the roll-out of GovAssure, BSI have service line to support organisations to close any gaps identified. The matrix below shows how our teams can support across the CAF Principles.



Cybersecurity services	Cloud security solutions	Vulnerability management	Incident management	Penetration testing/red teaming	Virtual CISO	TP security/ risk assessment
Information management and privacy	eDiscovery eDisclosure	Digital forensics	Legal tech	Data protection services	Data subject requests	DPO as a service
Security Awareness and Training	End user awareness	Phishing simulations	Social engineering	Certified Info tech training	Onsite and bespoke training	Online interactive solutions
Compliance services	PCI DSS	NIST	ISO/IEC 27001 management	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	⚪🔵⚫🔴	⚪🔵⚫🔴	⚪🔵⚫🔴	⚪🔵⚫🔴	⚪🔵⚫🔴	⚪🔵⚫🔴

6. Tips and recommendations

The key to this process is to identify the correct stakeholders and ensure that the resources are made available as needed for each of the critical services. The work should be set up as a formal project with milestones and a management sponsor to help with this.

The System owners are key stakeholders, and their input and engagement are considered essential. Raising awareness around GovAssure and the CAF amongst system owners and appropriate individuals / teams as early as possible will support those involved in the completion of the CAF self-assessment.

It is useful to view this as the first stage of an ongoing process. If evidence is not available, or the controls are not implemented, then this should be added to the list of non-compliance to address longer-term in the Get Well Plan (Step 5).

Four key tips for success

- Take time to fully understand the scope of the critical systems. This will make the responses to the IGPs more straightforward.
- Ensure any centralised controls (e.g. Governance) are documented before requesting local-level or technology-specific responses. This will prevent repetition of work.
- Provide a series of example responses and evidence tailored to your department systems and language. This will make the process smoother and more consistent across departments.
- Use the process to highlight known issues and risks. The scheme should be seen as a way to get more support to close gaps and remediate vulnerabilities.

The purpose of the initial GovAssure work is to provide the Cabinet Office’s Government Security Group (GSG) greater visibility of the common cyber security challenges facing government. Therefore, the key is to provide an accurate view of the current status, so that the risks can be properly understood and prioritised.