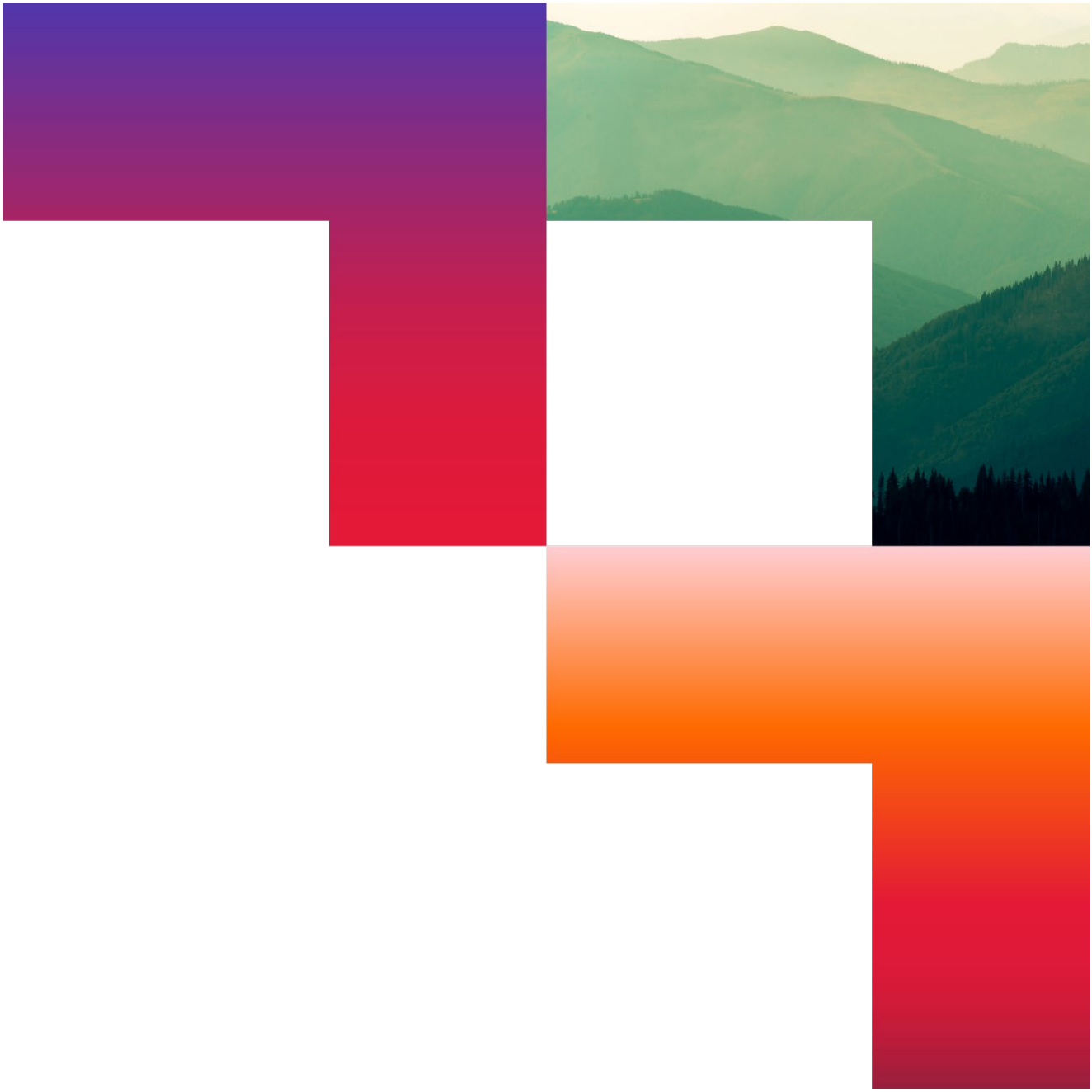


Cyber Assessment Framework (CAF) Assessment

Contracting body

30 Jan 2026

Issue 1.0

Table of contents

Service Definition overview

The Cyber Assessment Framework (CAF), developed by the National Cyber Security Centre (NCSC) the national technical authority for cyber security in the UK, provides a structured and comprehensive approach for assessing cyber risks to essential functions and the systems that support them. Originally designed to support organisations operating Critical National Infrastructure and to meet the requirements of the NIS Regulations, CAF has since proven to be a highly effective assurance framework for organisations across all sectors.

Our Cyber Assessment Framework (CAF) service helps organisations understand what “good” looks like in practice by assessing their arrangements against CAF’s four high-level objectives, 14 principles and 41 Indicators of Good Practice. The outcome provides a clear, evidence-based view of current cyber resilience and identifies, practical, prioritised improvements needed to strengthen the organisation’s ability to prevent, detect and respond to cyber threats.

Why CGI?

For more than 40 years, CGI has supported government and commercial organisations in securing their critical systems and delivering some of the most complex technology programmes and services. Our Cyber Assessment Framework (CAF) offering builds on this heritage, combining deep security management expertise with a comprehensive portfolio of cyber security services to provide clients with clear, actionable assurance.

CGI’s cyber security specialists bring significant in-house capability in cyber maturity assessment, including experienced and credentialed interviewers who have delivered CAF-aligned assessments across a wide range of organisations and sectors. Drawing on knowledge from both public and private sector environments, we help clients understand their current level of cyber resilience and identify practical steps to achieve the Indicators of Good Practice across the CAF objectives.

1. Service Description

The CAF is built upon a set of 4 objectives, 14 principles and 41 Indicators of Good Practice (IGP's), fed by contributing outcome statements.

We provide knowledge and expertise from across industry and public sectors to assess how your essential services achieve those indicators of good practice.

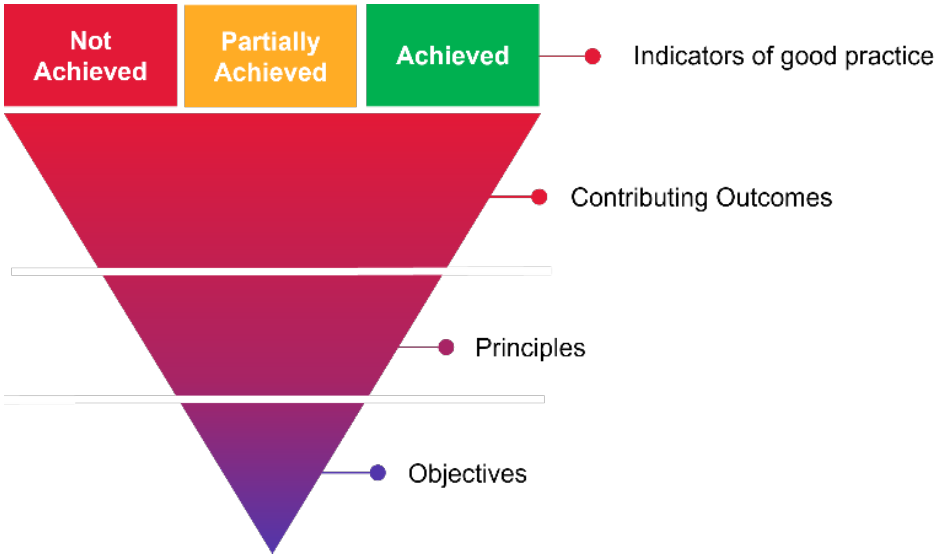


Figure 1. Cyber Assessment Framework

Each Cyber Assessment Framework (CAF) engagement begins with a structured scoping phase to ensure the assessment is focused on the organisation's essential function(s) and the network and information systems that support them. This includes consideration of the lifecycle stage of the function(s), such as whether services are in development, live operation, or transition. The agreed scope, including explicit in-scope and out-of-scope elements, is formally documented prior to assessment commencement.

Once scope is agreed, CGI conducts a comprehensive CAF assessment to determine how the organisation meets the CAF objectives, principles and IGP's. This is achieved through a systematic comparison of the organisation's security arrangements against the NCSC Indicators of Good Practice. Each IGP is assessed using CAF's defined outcomes of Achieved, Partially Achieved, or Not Achieved, supported by evidence and professional judgement.

The assessment is delivered through structured interviews led by experienced CGI cyber security specialists. Interviews are typically conducted in person but can also be facilitated securely via video conferencing where required. During the assessment, the interviewer guides nominated representatives through all 41 contributing outcomes, capturing relevant evidence, explanations and supporting artefacts to substantiate each assessment decision.

Following completion of the interviews, the assessment is consolidated, reviewed for its quality and formally approved to produce an authoritative, point-in-time view of the organisation's cyber resilience for the scoped essential function(s). A tailored post-assessment report is then provided, summarising the outcomes and presenting a prioritised, high-level action plan to address identified cyber resilience gaps and support ongoing improvement.

2. Methodology

The assessment is delivered by experienced CGI cyber security assessors, who work closely with nominated client representatives to plan and conduct the assessment activities. Depending on the scope and complexity of the essential function(s), the assessment may be conducted through a single interview or a structured series of interviews involving stakeholders relevant to the CAF objectives and principles being assessed.

Prior to commencing the assessment, the scope and parameters are formally agreed and documented. This includes, as a minimum:

- Client organisation
- Essential Function(s) in scope
- Assessment framework (NCSC Cyber Assessment Framework v4.0)
- Assurance context (GovAssure)
- Assessment period
- Report version and date
- Assessor(s)
- Distribution and handling requirements.

Once scope is confirmed, the assessment proceeds on a principle-by-principle basis. For each principle, assessors begin with a high-level, open-ended question designed to establish an initial understanding of how cyber resilience is achieved in practice for the essential function(s), and to gauge confidence in the effectiveness of existing arrangements.

As the assessment progresses, assessors explore areas in greater depth through targeted follow-up questions and, where appropriate, requests for supporting artefacts or evidence. This enables the assessor to corroborate statements made during interviews and to form evidence-based judgements. All information gathered during this process is captured within the CAF assessment toolkit and is reflected in summary in the final report.

	Section	High Level Questions
A1. Governance	A1.a Board Direction	How is security management led at board level, and how is this reflected in policy and decision-making?
	A1.b Roles and Responsibilities	How are roles and responsibilities for the security of networks and information systems defined across the organisation, and how are risks communicated and escalated when required?
	A1.c Decision-making	How is senior-level accountability for security decision-making established, and how are risks to essential function(s) considered alongside other organisational risks?

Figure 3. Snapshot of High Level, opening questions

Alongside the CAF assessment, the interviews are conducted in a manner that enables professional discussion regarding the consistency, sustainability and effectiveness of practices. Where appropriate, assessors may apply a CMMI-inspired maturity view to provide additional insight into the maturity of practices supporting each Indicator of Good Practice. This maturity view is supplementary, supports continuous improvement discussions, and does not form part of the formal CAF outcome.

Each of the four CAF objectives is assessed through structured evaluation of the contributing outcome statements using true or false responses supported by evidence. These contributing outcomes are used to determine the overall CAF outcome for each Indicator of Good Practice. Visual summaries of outcomes are generated within the toolkit and used to support both assessment review and reporting.

Details of all interviews conducted, along with references to supporting artefacts and evidence, are formally recorded within the assessment toolkit. Upon completion, the assessment is reviewed, validated and approved, resulting in a controlled, point-in-time record of cyber resilience for the scoped essential function(s).

Finally, the outcomes of the assessment are presented both within the completed CAF toolkit and through a formal assessment report. The report includes an executive summary, a clear articulation of assessment outcomes, and a high-level, prioritised action plan to support the management and improvement of cyber resilience.

3. Data Backup and Restore

CGI can carry out backup and restore activities in accordance with any specific requirements and in compliance with the Information Assurance Backup / Restore policies as defined in ISO 27001; any information that has

been processed as part of an engagement will be stored securely. Where applicable, this information can then be restored from an appropriate back-up.

4. Service Continuity

CGI will agree appropriate service continuity in accordance with any specific requirements, and any conditions that need to be met.

5. Onboarding and Offboarding

5.1. Onboarding

For Specialist Cloud Services, CGI will engage directly with the client to ensure the full scope of the requirements is understood and agreed in advance of any engagement. We will work with senior stakeholders to define the necessary business outcomes and ensure the services are aligned accordingly.

For all services, CGI understands the client's requirements and make on-boarding specific to these needs, using the experience, lessons learnt and methodology from many years of public sector transition experience, we can quickly align to client joiners, movers and leavers policies and ensure that we have appropriately cleared staff for every engagement.

5.2. Offboarding

Off-boarding is instigated by a client request or after expiration of the service agreement.

5.2.1. Access to data upon exit

Deletion of any virtual machine image and data will occur in line with the service agreement. Any required data will be made available using appropriate media, in line with the data security classification. After client notification that data has been successfully recovered, CGI will purge and destroy client data from any computer or storage device or media that remains part of CGI's estate, with the exception of any data related to a data retention agreement between a client and CGI.

6. Service constraints

CGI will work with you to define and tailor the services to meet your specific requirements. During this definition period, detailed responsibilities will be agreed across the service delivery. Examples of common general constraints are listed below:

- Share the existing internal sponsorship and governance for Information Assurance.
- Assign or appoint a suitably skilled and empowered person to act as the receiving client.
- Provide appropriate access to its policies, processes and standards for the Information Assurance service and other suppliers.
- Provide timely information relating to its business plans, goals and projects.

As a main feature of any Service will necessitate an on-going dialogue with client representatives, the most important responsibility of the Contracting Body is to ensure the timely availability of individuals for fact-finding interviews.

7. Service levels

The overall accountability for the relationship with the client lies with CGI’s Executive Sponsor and CGI Account Manager and they will provide strategic governance to the service working closely with the client's Senior Executive team or nominated delivery / engagement contact. The purpose of this team is to ensure that the

relationship is collaborative, the service is delivering, as agreed, the governance model is working, and best practice is being applied.

8. Hosting options and locations

CGI has a network of 21 offices across the United Kingdom and Northern Ireland, with our UK members having the capability to deliver as hybrid-workers. Through our engagements we also understand that for some clients it is essential that our members are physically present on their sites, our distributed network of offices makes this possible. Whatever your requirements are the options for hosting and locations will be agreed at contract negotiations.

9. Security

CGI has invested significant resources to develop an Enterprise Security Management Framework (ESMF) based on recognized industry standards and applicable regulations or legislation such as ISO 27001, ISO27701, NIST, COBIT, CIS, CCPA and GDPR to name but a few. This framework is used across the global organization to protect information assets, technologies, facilities, and CGI members, including the data managed across the business, and is supported by CGI's security and privacy policies, standards and controls (Security Baseline) which are implemented through our processes, practices, services, solutions and our interactions with any third parties working on behalf of CGI.

Across the CGI business, the technical and organizational measures are defined using a risk-based approach. This considers the nature, scope, context and purposes of processing as well as the risk to the rights and freedoms of natural persons, where CGI is acting as either the data controller or data processor. This ensures a level of security and privacy appropriate to the risk, in situations where CGI holds responsibility and accountability for personal data processing.

CGI's ESMF Security Baseline is the minimum-security standard for all CGI offerings (including cloud-based services) to be applied by both CGI and clients. In some cases, CGI Security or Data Privacy may wish to add additional controls e.g. where sensitive personal data is involved. Where CGI or our clients agree to strengthen the level of security or privacy to consider specific requirements (risks, regulatory requirements, etc.) these additional security or protective measures will be defined within the CGI contracted services, particularly where CGI may be acting as data processor on behalf of a client.

10. Service Pricing and Terms and Conditions

10.1. Pricing

Please refer to the G-Cloud 15 portal for the rates available.

10.2. Terms and Conditions

Please refer to the associated Terms and Conditions Document relevant for this Service including termination by the Buyer or Supplier.

11. Further information

For more information about this or any of our G-Cloud services, please contact us:

We will prepare a quotation for you. Once the quotation is agreed upon, we will issue you the necessary documentation (as required by the G-Cloud

Phone: +44 0845 070 7765. Ask to speak to the G-Cloud team.

Email: uk.gen.ccsframeworks@cgi.com, including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

Framework) and ask you to provide us with a purchase order.

Once we have received your purchase order, the services will be configured to the requirements agreed with invoices issued to you for the services procured. On a monthly basis, we will also complete the mandated management information reports to Government Procurement.

PROPRIETARY AND CONFIDENTIAL

The information in this proposal is submitted on 30 Jan 2026 - Issue 1.0 on behalf of CGI by the following authorised representative:

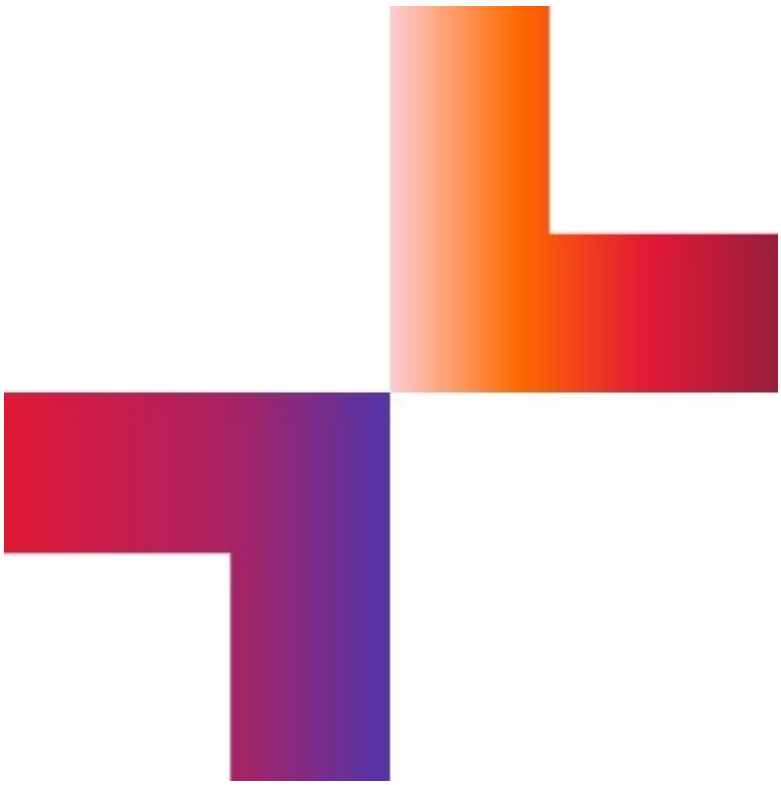
Simon Figg

Frameworks Manager

CGI IT UK Ltd

14th Floor, 20 Fenchurch Street, London, EC3M 3BY

Tel: +44 0845 070 7765



cgi.com/uk