



Cyber Security Strategy

Contracting body

30 Jan 2026

Issue 1.0

© 2026 CGI IT UK Ltd

CGI

Table of contents

1.	Service Description	4
1.1.	Key challenges addressed by a Cyber Security Strategy include:	4
1.2.	Benefits of a Cyber Security Strategy	4
1.3.	Service Delivery and Approach	5
2.	Data backup and restore	5
3.	Service Continuity	5
4.	Onboarding and Offboarding	5
4.1.	Onboarding	5
4.2.	Offboarding	6
5.	Service constraints	6
6.	Service levels	6
7.	Hosting options and locations	6
8.	Security	6
9.	Service Pricing and Terms and Conditions	7
9.1.	Pricing	7
9.2.	Terms and Conditions	7
10.	Further information	7
PROPRIETARY AND CONFIDENTIAL		8

Service Definition overview

A Cyber Security Strategy provides a structured, risk-based approach to protecting an organisation's information assets, systems, and services against an evolving and increasingly sophisticated cyber threat landscape. It establishes a clear framework for how cyber risks are identified, prioritised, and managed in line with business objectives, enabling informed decision-making and effective governance at executive and board level.

For UK-based organisations, an effective cyber strategy supports compliance with key regulatory and policy frameworks, including UK GDPR, the Network and Information Systems (NIS) Regulations, and relevant government security standards. Beyond compliance, it helps organisations demonstrate accountability, resilience, and due diligence, ensuring that cyber security investment is proportionate to risk and aligned to organisational priorities.

For organisations operating internationally, cyber strategies must also address a broader and more complex regulatory and threat environment. This includes alignment with EU legislation such as EU GDPR and the NIS2 Directive, as well as applicable global cyber security standards. A coherent strategy enables a consistent security posture across multiple jurisdictions while allowing for local regulatory, operational, and cultural differences.

CGI's Cyber Strategy service draws on decades of experience delivering secure digital solutions across public and commercial sectors. Our approach integrates business drivers, regulatory obligations, threat intelligence, and existing security capabilities to develop pragmatic and actionable cyber strategies. These strategies are tailored to organisational risk appetite and maturity, providing a clear roadmap that prioritises initiatives, supports sustainable improvement, and strengthens long-term cyber resilience.

The outcome is a cyber strategy that not only protects critical assets and services, but also supports digital transformation, enables innovation, and provides confidence to stakeholders that cyber risk is being managed effectively and responsibly.

Why CGI?

For over 40 years, CGI has helped secure government and commercial clients and delivered some of the most complex technology projects and services. Thanks to this experience, we bring accelerators in the form of maturity models, reference architectures, technical know-how, cross-domain expertise, risk management methods, and client lessons learned to accelerate and empower your business.

CGI's Cyber Security has significant in-house expertise in delivering cyber security services for a wide variety of organisations, ranging from highly sensitive government departments, through regulated industries, to large commercial enterprises and technology-oriented entrepreneurial businesses.

1. Service Description

In an increasingly digital and interconnected environment, organisations are heavily reliant on technology to deliver services, improve efficiency, and enable innovation. The adoption of cloud computing, remote working models, digital supply chains, and data-driven services has significantly expanded the cyber-attack surface, increasing exposure to both targeted and opportunistic threats.

Cyber security incidents now pose material risks to operational resilience, financial stability, regulatory compliance, and organisational reputation. Threat actors continue to evolve their tactics, exploiting vulnerabilities across people, processes, and technology, while supply chain compromise and ransomware remain prevalent across all sectors.

In response, cyber security regulation and guidance has strengthened across the UK and internationally. In the UK, organisations are expected to align with frameworks such as the NCSC Cyber Assessment Framework (CAF), ISO/IEC 27001, **emerging cyber resilience legislation** and sector-specific regulations including the NIS Regulations. For organisations operating within the EU, equivalent obligations arise under EU GDPR, the NIS2 Directive, and local Member State cyber security requirements.

A Cyber Security Strategy provides a clear roadmap for managing these risks. It establishes a current-state understanding of cyber maturity, defines a target security posture aligned to business objectives and regulatory expectations, and sets out a prioritised improvement plan to address identified gaps.

CGI works with clients to develop cyber strategies that are proportionate, achievable, and sustainable. Our approach recognises that cyber security is not solely a technical challenge, but a business risk that requires executive ownership, effective governance, and sustained investment to support long-term organisational resilience.

1.1. Key challenges addressed by a Cyber Security Strategy include:

- Increasing frequency and sophistication of cyber attacks, including ransomware and supply chain compromise.
- Regulatory compliance across UK and EU cyber and data protection frameworks.
- Inconsistent security controls across legacy, cloud, and third-party environments.
- Limited visibility of cyber risk at executive and board level.
- Skills shortages and unclear accountability for cyber security ownership.
- The need to balance security investment with business agility and innovation.

1.2. Benefits of a Cyber Security Strategy

Beyond regulatory compliance, an effective Cyber Security Strategy delivers tangible business benefits, including:

- Improved protection of critical services and sensitive data.
- Reduced likelihood and impact of cyber security incidents.
- Clear executive and board-level visibility of cyber risk.
- Improved alignment between cyber security investment and business priorities.
- Greater confidence in the security of third-party and supply chain relationships.
- Enhanced organisational resilience and readiness for regulatory scrutiny.

For organisations with operations across multiple jurisdictions, a well-defined cyber strategy also ensures a consistent and defensible security posture across the UK, EU, and other international markets, while accommodating local regulatory and operational requirements.

1.3. Service Delivery and Approach

CGI delivers Cyber Security Strategy engagements through a structured and collaborative approach aligned to business objectives, regulatory obligations, and recognised UK and international best practice. As part of our Cyber Strategy service, CGI will:

- Assess the current cyber security maturity across people, processes, policies and technology
- Identify key cyber risks and threat scenarios relevant to the organisation
- Review alignment with UK regulatory, policy, and industry frameworks
- Consider EU and international regulatory requirements where applicable
- Define a target cyber security operating model and control framework
- Develop a prioritised, cost-effective roadmap aligned to business objectives
- Support the integration of cyber strategy into enterprise risk management and transformation programmes

Phase 1 – Initiation and Scoping

Confirm strategic objectives, scope, stakeholders, and applicable UK and international regulatory requirements.

Phase 2 – Current State Assessment

Assess existing cyber security maturity across people, processes, Policies and technology against recognised frameworks.

Phase 3 – Risk and Gap Analysis

Identify and prioritise cyber risks and control gaps based on the organisation's threat landscape and risk appetite.

Phase 4 – Target State Definition

Define a pragmatic target cyber security posture aligned to business goals and regulatory expectations.

Phase 5 – Roadmap and Investment Planning

Develop a prioritised and cost-effective roadmap to transition from current to target state.

Phase 6 – Strategy Documentation and Executive Engagement

Produce a clear Cyber Security Strategy and roadmap to support executive decision-making and governance.

2. 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, should the need arise.

3. Service Continuity

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

4. Onboarding and Offboarding

4.1. 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.

4.2. Offboarding

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

4.2.1. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. Service Pricing and Terms and Conditions

9.1. Pricing

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

9.2. Terms and Conditions

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

10. Further information

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

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.

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 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 contained in this document is confidential to CGI and/or CGI group companies. This document shall not be reproduced in any form or by any mechanical or electronic means, including electronic archival systems, or submitted to a generative AI tool without the prior written approval of CGI. The receiving party may use this document and the information contained in it for the purpose of evaluating CGI's proposal only. Any personal data included in this document must not be replicated, stored or distributed beyond the immediate recipient or used for any purpose other than evaluating the document.

This proposal is subject to contract and shall not be binding unless and until execution by CGI and Contracting body of a final agreement to the proposal, containing the terms and conditions that will govern the relationship between the parties. Any final agreement is conditional (inter alia) upon due diligence and customary business investigations by CGI. The results of such due diligence and/or investigations may impact upon content of this proposal, including the business structure, business terms and financial arrangements.

If you have received this document by mistake, note that the reading, the reproduction or the distribution of this document is strictly forbidden. You are hereby requested to inform us by telephone at +44 0845 070 7765 and to return this document by special delivery marked for the attention of Simon Figg.

Except where indicated otherwise, all names, trademarks, logos and brands (registered or not) referred to in this document are the property of a company in the CGI group or its licensors.

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

