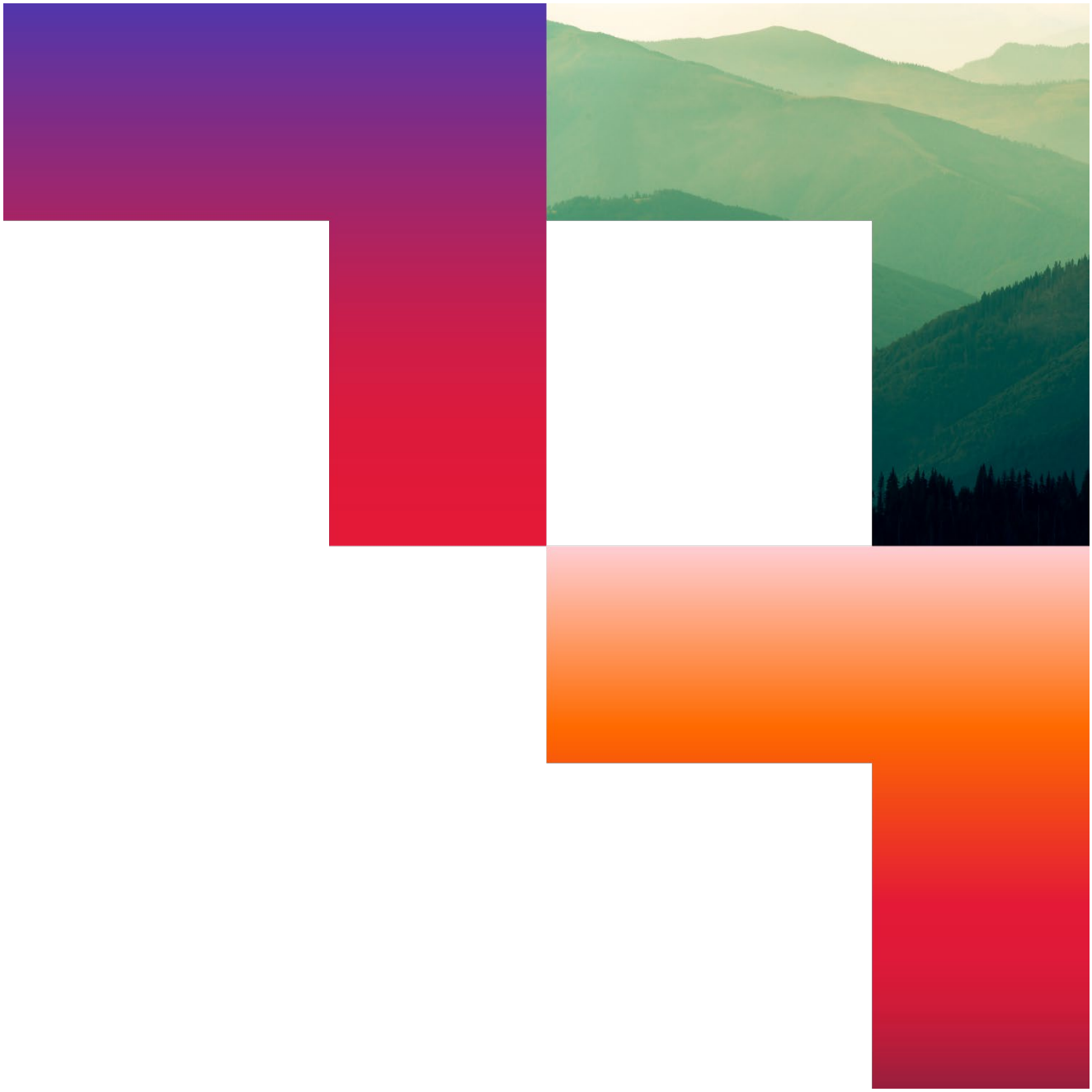


Cyber Security in the Supply Chain

Contracting body

30 Jan 2026

Issue 1.0

Table of contents

Service Definition overview

Today’s organisations depend on a vast network of external suppliers and partners to deliver critical products, systems and services. With the rapid adoption of digital technologies such as cloud computing and AI, supply chains have evolved into highly complex, interconnected ecosystems. While this transformation brings efficiency and innovation, it also introduces new security risks at every link in the chain.

Protecting the confidentiality, integrity and availability of information across these networks is no small feat. Data and services often span multiple environments—across business units and third-party organisations—each with their own security controls and risk appetites. Vulnerabilities can emerge during supplier onboarding, throughout the lifecycle, and even deep within sub-supplier tiers.

To stay ahead of these challenges, organisations need a structured, end-to-end approach to regularly managing supply-chain cyber risks. This means identifying weaknesses, prioritising threats, and building resilience across every tier.

CGI’s Cyber Security in the Supply Chain service provides exactly that. Our pragmatic, risk-based methodology delivers a clear picture of supplier-related cyber risks and a practical roadmap to strengthen resilience. From comprehensive risk profiling to actionable strategies, we help you secure your supply chain against evolving threats—so you can focus on driving business forward with confidence.

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

The Emerging Threat

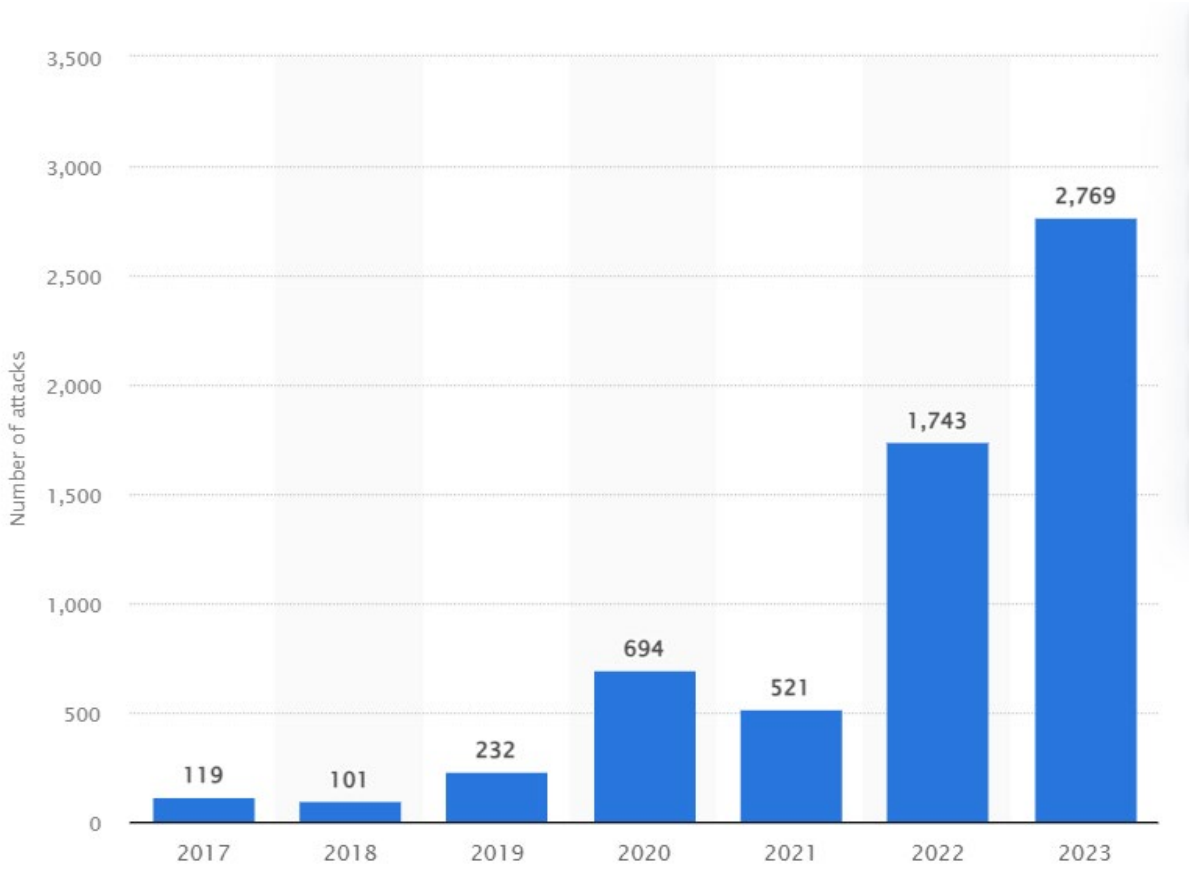
Figure 1

In recent years, supply-chain cyber risk has become one of the most significant enterprise threats for organisations worldwide. Latest industry reporting shows that more than 70% of organisations experienced at least one significant third-party or supply-chain security incident, with a notable portion experiencing multiple incidents over the past year. Despite this prevalence, fewer than half of organisations monitor cybersecurity across most of their extended supply chain, and only a quarter integrate incident response planning into their third-party risk management programmes.

These figures illustrate the ongoing challenge organisations face in gaining visibility and control over supplier-related cyber risk. As supply chains grow more interconnected, spanning internal teams, outsourced partners, cloud providers, and digital service ecosystems, the likelihood and potential impact of compromise increase accordingly.

Managing supply-chain cyber risk is therefore a critical part of organisational resilience, affecting operational continuity, data protection, regulatory compliance, and stakeholder confidence.

Table 1. Annual Numbers of Supply Chain attacks in the United States from 2017 to 2023



(Source: https://www.statista.com/statistics/1367208/us-annual-number-of-entities-impacted-supply-chain-attacks/)

The Weakest Link

An organisation's supply-chain security is only as strong as its least secure supplier. Modern supply chains are increasingly global, complex, and multi-tiered, drawing on diverse sources of software, services, and components. This complexity introduces inherent vulnerabilities that can be exploited by cyber threat actors targeting third-party software providers, development platforms, website builders, and data repositories. Such

attacks can result in data breaches, service disruption, and the loss of sensitive information, including customers' intellectual property.

When selecting and managing suppliers, organisations face a range of cyber risks, including business impersonation, counterfeit or unauthorised software, unstable or unsupported products, and hidden vulnerabilities such as malicious code injection or dependency confusion. These risks may be introduced at onboarding or emerge over time as supplier services and dependencies evolve.

Despite the growing threat, many organisations still lack comprehensive visibility of the security posture across their supply chains. UK government cyber security surveys have consistently shown that while larger organisations are more likely to review immediate supplier risks, systematic supply-chain risk assessment remains limited across the wider business population.

Supply-chain compromise has become an increasingly attractive attack vector for cyber threat actors. Industry bodies and national cyber authorities, including SANS and the European Union Agency for Cybersecurity (ENISA), continue to highlight supplier vulnerabilities as a major contributor to cyber incidents, reinforcing the need for structured third-party risk management and ongoing assurance throughout the supplier lifecycle.

The Challenges

Whilst this problem can be understood, the interconnected and distributed nature of a supply chain can make it difficult to know how your suppliers are managing and maintaining their cyber security. Organisations with limited resources may face challenges such as:

Figure 2.

- Low understanding of the risk that poor supply chain cyber security can pose.
- Limited visibility into supply chain vendors and entities
- Insufficient tools and expertise to evaluate a supplier's security posture.
- Not knowing what to ask suppliers to meet a high security standard.

This highlights the importance of understanding and managing supply chain cyber security risks. It also emphasises the challenges organisations may face, especially those with limited resources. It's crucial for these organisations to recognise these risks and invest appropriately in their mitigation. This includes gaining visibility into their supply chains, supporting them with the necessary tools and expertise, and knowing the right questions to ask their suppliers.

Do you fully understand the security of your entire supply network?

How aware are you of each supplier's security posture, policies, and processes?

Are they meeting global security standards, regulations, and legal requirements?

What data do you share with your supplier? Is it being stored and transferred securely?

Are you confident your supplier could continue to support your business in the event of a breach?

What is a Supply Chain?

In general terms we often think of a supply chain as a network of entities involved in the production, distribution, and delivery of products or services from a supplier to an end customer or business. Qu**ite often these entities interact with each other to allow the chain to function effectively. For most organisations each entity plays a vital role and can be crucial to supporting their everyday business operations.**

In today's operating environment, the supply chain represents an interconnected ecosystem of suppliers, service providers, technologies, and people that collectively enable products and services to be delivered, operated, and supported. These dependencies are tightly coupled, meaning disruption, failure, or compromise in one area can quickly cascade across others.

Within this ecosystem, organisations rely on a wide range of commercial, operational, and technology dependencies that can directly or indirectly influence business outcomes. These must be understood and managed as part of overall supply chain risk, and include areas such as:

- **Software & Engineering**
- Application code, open-source libraries, and third-party software components

- Build systems, CI/CD pipelines, and development tool**s**
- **Infrastructure & Platforms**
- Cloud service providers (IaaS, PaaS, SaaS)
- Industrial Internet of Things (IIoT), operational technology, and ICS
- Hardware, firmware, and device manufacturers
- **Data & Artificial Intelligence**
- External data sources, feeds, and APIs
- AI models, training data, generative AI, and AI as a Service (AIaaS)
- **People & Operations**
- Developers, operators, and privileged identities
- Credentials, keys, and trust relationships
- Managed services, monitoring, and incident response providers.

Why It Matters

- Security: Supply chain attacks can bypass traditional organisational controls
- Resilience: Failures or outages in one dependency can propagate across the ecosystem
- Compliance: Regulations increasingly target third-party and fourth-party risk
- Trust: Customers, partners, and regulators expect transparency and assurance.

Supply chain risk is business risk. Managing it requires visibility and control across code, platforms, data, people, and vendors — not just the applications you build or buy.

1.1. Service Delivery and Approach

At CGI, we recognise that organisations of all sizes typically have extensive and complex supply chain ecosystems. This is due to an increasing reliance on third-party providers for products and services, driven by the demand for advanced technology. These relationships often grant third parties both physical and logical access to data, proprietary information, and systems managed on behalf of the primary organisation.

This access inherently introduces additional security risks. It's crucial that these risks are identified, assessed, and managed through the implementation of suitable controls. This improves the protection of the organisation and enables its daily operations to proceed with confidence.

We offer a service called 'Cyber Security in the Supply Chain', which equips clients with the capabilities required to gain a comprehensive understanding of their supplier ecosystem. The service focuses on assigning criticality ratings to suppliers, identifying inherent and residual risks, and recommending a balanced and risk-based approach to strengthening security posture through appropriate protective controls. Our approach is informed by recognised international standards, best-practice guidance, and proven assessment techniques, enabling security assurance across the end-to-end business environment.

We equip our clients with tools to analyse supply chain data, helping them target high-risk areas. Our services extend beyond traditional logistics, storage, and distribution to secure elements of emerging technologies like cloud and artificial intelligence.

We employ a highly proactive approach to security which enables our clients to stay ahead of threats, rather than merely reacting to them.

We collaborate with our clients and their suppliers to ensure compliance with best practices and standards, particularly the ISO27001 and ISO28000 series. This demonstrates that despite the complexity of external threats, risks, new technologies, and myriad of regulations, the client organisation is equipped with a security-focused management structure.

Our security consultants are well-versed in security standards and will employ various methodologies to assess cybersecurity across the entire supply chain. For instance, our preferred risk assessment tool creates individual profiles for suppliers, ensuring the entire supply chain is identified. This tool features an interactive dashboard that can instantly respond to any changes input during the assessment, offering enhanced visibility and assurance of supply chain performance and risks. This enables our clients to make informed decisions about vendors and suppliers, evaluate decisions based on risk and compliance evidence, enhance supply chain

efficiency and productivity, and minimise supply chain disruptions. By Incorporating the National Cyber Security Centre's (NCSC) 12 Principle Supply Chain Security Guidance into the core of this service, we strive to provide practical steps to help our clients gain assurance within the security of their supply chain.

1.2. How We Do It

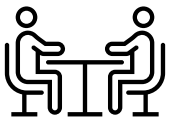
At CGI we align to the NCSC '12 Principle Supply Chain Security Guidance' which is designed to help organisations establish effective control and oversight of their supply chain network. These principles recognise that most organisations are reliant upon many suppliers to deliver products, systems, and services and this can often be large and complex. Therefore, we implement each of these principles in four comprehensive stages, listed below. Each principle embodied within the core of our service, and we work closely with our client and all their suppliers throughout each stage the supplier lifecycle.

Stage 1: Understand the Risks

- Understand what needs to be protected and why.
- Know who your suppliers are and build an understanding of what their security looks like.
- Understand the security risk posed by your supply chain.

In this stage we will correspond to these first three principles to carry out information gathering of our client's supply chain network. This includes an initial visit to identify all the parties within the supply chain, categorise their services and build criticality ratings based on the business impact. We then offer a blend of onsite supplier visits, virtual interviews, and online questionnaires to validate and further investigate the suppliers own cyber security policies, practices and procedures.

Stage 2: Establish Control



- Discuss the purpose of the security review with suppliers.
- Set and communicate minimum security requirements for suppliers.
- Build security considerations into contracting processes.
- Assist the supplier with meet the security responsibilities.
- Raise awareness of security within the supply chain.
- Provide support for security incidents.

In this stage we utilise principles 4-9 to help to gain and maintain control of the supply chain. Using our tailored methodology, we will be able to identify areas where there is a lack of security compliance within the suppliers and advise where risks are presenting weaknesses which may result in these risks are inherent. We will advise the prime supplier of any risks and provide proposals of areas for remediation and improvement. We can also work with the suppliers to implement improvements as required. We will aid in the event of a third-party breach and support incident investigations.

Stage 3: Check Your Arrangements

- Build assurance activities into your supply chain management.

We will provide a responsive dashboard that can be used as a security monitoring tool across the whole supply chain. This provides real-time indications of your whole supply chain security posture and includes periodic reporting of criticality and resilience levels. Periodic assessments will provide the necessary information to keep appraised of the security confidence and compliance accreditation within the supplier network.

Stage 4: Continuous Improvement

- Encourage the continuous improvement of security within your supply chain.
- Build trust with suppliers.

As your supply chain evolves, your relationship with them will need to continue to be collaborative and incorporate a bi-lateral agreement to the improvement and maintenance of cyber security. Here we use principles 11 and 12 to offer our commitment to provide a continued Cyber Security in the Supply Chain service. We offer periodic reviews to identify where implementation of improvements will increase levels of compliance against the new and evolving cyber security standards. We offer the on-going support and expertise of our highly experienced cyber security team to our clients and their suppliers helping to build

confidence and a commitment to working together to mitigate cybersecurity risks. We offer to help develop partnerships with your suppliers. If your suppliers adopt your approach to supply chain security as their own, there's much greater potential for success than if you simply mandate compliance.

1.3. Benefits

In today's digital age, where cyber threats are increasingly sophisticated and frequent, assessing the cybersecurity posture of a supply chain is not just beneficial, but essential. These are the benefits our clients enjoy when using our Cyber Security in the Supply Chain service:

- Better Awareness: Clearer understanding of the complexity of their whole supply chain, including their associated risk and criticality.
- Identify Vulnerabilities: Identifying potential vulnerabilities and weak links in the supply chain that could be exploited by cybercriminals.
- Risk Mitigation: Mitigate risks associated with their suppliers and reduce exposure to potential cyberattacks.
- Improved Security Measures: Improved security measures and protocols, thereby strengthening the overall cybersecurity posture.
- Trust and Confidence: Build trust and confidence among stakeholders, including customers and partners, as they can be assured of the security of their data.
- Compliance: Ensure compliance with regulatory requirements related to data protection and privacy.
- Proactive Defence: Be proactive rather than reactive in dealing with cybersecurity threats.
- Continuous Monitoring: A real-time view of each supplier’s security posture, allowing for timely risk assessments.
- Raise Awareness: Establish supply chain security management training for appropriate staff.

1.4. Information Assurance

Management Foundation

CGI operates a proprietary Management Foundation underpinned by an Integrated Management System (IMS) for information assurance and service delivery. Our IMS processes are independently certified to recognised international standards, including BS EN ISO 9001.

CGI is committed to maintaining its UK-based certifications and accreditations and extending these where required to meet client and regulatory expectations. The CGI Management Foundation is designed to incorporate best practice drawn from across public sector and commercial engagements.

Our accreditations include:

- ISO 9001:2015
- ISO/IEC 20000-1 (IT Service Management)
- ISO/IEC 27001:2022 (Information Security Management)
- ISO/IEC 22301:2019 (Business Continuity Management)
- SSAE 18 / ISAE 3402 assurance reports (where applicable)
- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
- Microsoft Intelligent Security Association Member
- Member Chartered Institute of Information Security (CIISec).

Information Classification and Sharing

Information is managed at an appropriate security classification for each service. CGI-hosted services can support information classified in accordance with the UK Government Security Classification (GSC), subject to service scope and assurance requirements.

CGI supports clients in meeting incident reporting obligations under UK GDPR, including notification to the Information Commissioner’s Office within statutory timescales where applicable. We also promote responsible information sharing across supply chains to improve collective awareness of emerging threats. Participation in initiatives such as the Cyber Security Information Sharing Partnership (CiSP) is encouraged.

Information Principles for the UK Public Sector supported and documented?

CGI recognises the UK Public Sector information principles which are fundamental to the efficient and effective delivery of public services. Where we store and manage government information in our GCloud services we aim to ensure that it is appropriately protected and available to exploit. Through this we would aim to maintain and, depending on the service purchased, enhance the quality of the information stored in a standard manner that enables its re-use. Where the selected services require it, we would engage positively both to support the buyer in the publication of public information and to support them in the access of information by citizens and business.

Government ICT Strategy and Greening Government ICT Strategy supported and documented?

The design and delivery of our Cloud-based SaaS offerings is consistent with the principles of the Greening Government ICT Strategy. Scalable, Cloud-based services allow pooling of capacity across multiple clients, reducing overall hardware requirements. These are further reduced through virtualisation, which has delivered up to a 90% reduction in server numbers and power consumption for some of our services. We select modern, energy efficient servers, storage and network hardware and have also invested heavily in improving the energy efficiency of our data centres. This includes initiatives such as free air cooling, aisle containment, power supply upgrades, lighting controls and power management and monitoring software. In the UK, electricity for our data centres is sourced from renewables, which is also the case for many of our third-party hosting providers. We closely manage the impact of IT hardware throughout its lifecycle, aiming to optimise refresh cycles to balance in-use carbon savings of newer, more efficient hardware against the carbon impact of its manufacture. At end of life, we also ensure responsible disposal through resale or recycling of old hardware wherever possible. Our sustainability performance has won widespread recognition, including our listing on the Carbon Disclosure.

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

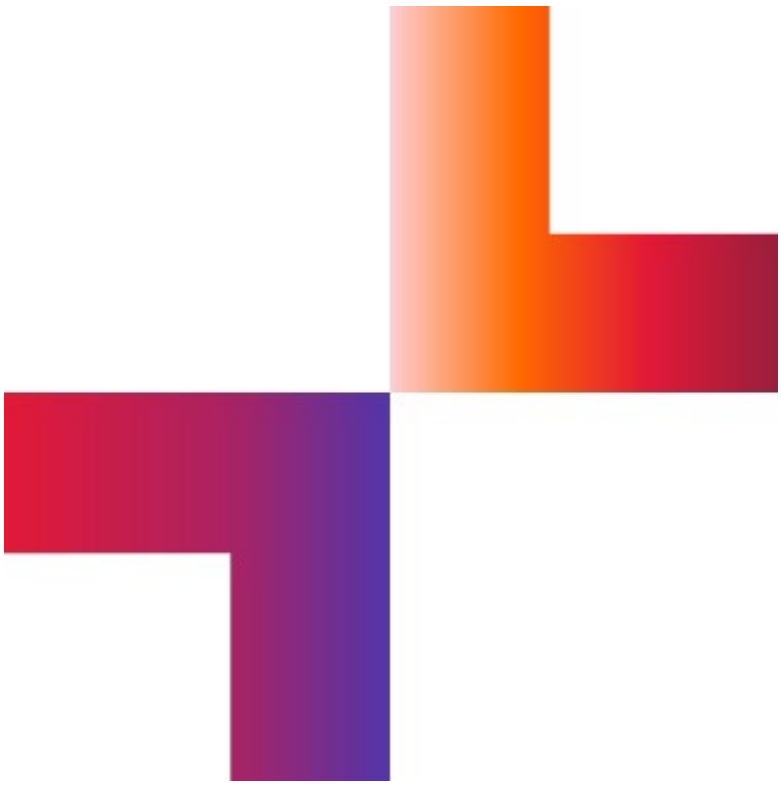
Simon Figg

Frameworks Manager

CGI IT UK Ltd

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

Tel: +44 0845 070 7765



cgi.com/uk