



Vulnerability and Remediation Management

Contracting body

30 Jan 2026

Issue 1.0

© 2026 CGI IT UK Ltd

CGI

Table of contents

1.	Service Description	4
1.1.	Service Features	4
1.2.	Service Benefits	4
2.	Service Continuity	4
3.	Onboarding and Offboarding	5
3.1.	Onboarding	5
3.2.	Offboarding	5
4.	Service Constraints	5
5.	Service Levels	5
6.	Technical requirements	5
7.	Security	6
8.	Service Pricing and Terms and Conditions	6
8.1.	Pricing	6
8.2.	Terms and Conditions	6
9.	Further information	6
PROPRIETARY AND CONFIDENTIAL		8

Service Definition overview

CGI's Vulnerability and Remediation Management services are instrumental in empowering organisations to fortify their cybersecurity defences. By identifying, prioritising, and addressing security weaknesses within their Public or Private cloud hosted systems, networks, and applications, CGI helps clients proactively mitigate cyber threats and safeguard sensitive data and assets.

The cyber threat landscape continues to evolve with new, innovative, and varied attack methods adapting to their chosen targets environments and driving the threat world into new areas. The risks to your organisation from cyber security incidents is real, and attacks regularly cause significant damage to the performance and reputation of many organisations.

Vulnerability assessment and remediation patching, in conjunction with continuous 24x7x365 protective monitoring, helps you identify issues and rectify them before they do considerable damage to your organisation. These critical security services overlay and augments traditional defences with critical sources of information, improving network visibility and security.

CGI's vulnerability and remediation management services empower organisations to fortify their cybersecurity defences. By identifying, prioritising, and addressing security weaknesses within their systems, networks, and applications, CGI helps clients proactively mitigate cyber threats and help to safeguard sensitive data and assets.

Our comprehensive vulnerability and remediation service equips organisations with the necessary tools, insights, and support to effectively identify and remediate security vulnerabilities. By reducing cyber risk and enhancing their overall cybersecurity posture, CGI enables organisations to confidently navigate today's evolving threat landscape.

Why CGI?

CGI has been a leading security service provider with over 40 years of experience in managing risk efficiently and effectively. With a firm focus on delivering optimal value for money, we combine our deep industry experience and partner network with innovative technology to provide trusted, reliable cloud platforms and cost-effective security solutions for protecting your services and data.

We have a long-standing and highly regarded reputation in IT and business consulting. We offer managed services across a wide range of sectors including commercial, education, financial, insurance, central government, and critical national infrastructure. Individual reference points are available upon request.

We help businesses and government clients to assess risks, protect their business and operate with confidence in the digital world. Over 80% of our team of 1,700 cyber security professionals have government clearances. We operate from 10 Security Operations Centres globally to deliver cyber security services that are tested and proven in some of the world's most sensitive and complex environments.

As an experienced managed security services provider (MSSP), CGI provides clients with the expertise and capabilities required to implement and operate highly secure infrastructures, focusing on:

- Governance, risk, and compliance to increase regulatory compliance and reduce audit costs and findings.

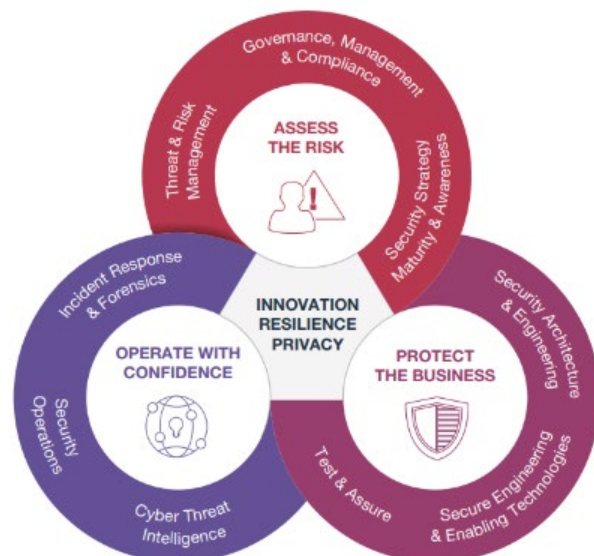


Figure 1 - CGI in Security services

- Risk management to protect information and critical assets and ensure confidentiality.
- Infrastructure protection management to deliver the latest security network and systems technologies.

We have invested heavily in establishing our credentials, working closely with international security associations and standards bodies. Our global experience helps us predict and defend against new attacks, and our front-line capabilities reflect this knowledge.

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world. We are insights-driven and outcomes-based to help accelerate returns on your investments. Across 21 industry sectors in 400 locations worldwide, our 94,000 professionals provide comprehensive, scalable, and sustainable IT and business consulting services that are informed globally and delivered locally.

1. Service Description

CGI's Vulnerability and Remediation Management (VAR) service, frees you from the burden of network discovery and vulnerability identification. Our VAR Team prioritises risks based on the impact to your business, ensuring you can address them efficiently. We report all this data in an actionable format to your relevant working groups, empowering you to take prompt action.

Once configured for your environments, our industry-leading vulnerability monitoring tools effectively detect and inventory assets across your global hybrid-IT cloud environments, including physical / virtual servers and network devices like firewalls and load balancers.

1.1. Service Features

- Conduct regular vulnerability scans (typically 4 hrs) of IT infrastructure to identify potential vulnerabilities.
- Threat intelligence feeds to understand emerging threats and vulnerabilities.
- Remediation planning and guidance to address identified vulnerabilities.
- Routine patch scheduling and management (emergency, monthly, quarterly).
- Compliance support for regulatory requirements and industry standards.

1.2. Service Benefits

- Enhanced overall security posture.
- Reduced exposure to cyber risks and better data protection.
- Demonstrate compliance with relevant regulations and standards.
- Minimise system downtime, avoid disruptions to business operations.
- Enhance customer trust, strengthen brand reputation.
- Avoiding costs associated with data breaches and regulatory fines.

2. Service Continuity

CGI has extensive experience of BCDR planning and requirements, including for several government agency clients, supporting critical national infrastructure systems. As part of a continued commitment to maintaining ISO27001:2013 certification, CGI maintains an overall Business Continuity Plan and a supporting plan structure. This incorporates IT Disaster Recovery (ITDR) and IT Service Continuity (ITSC) plans as part of our Information Security Management System. CGI operates a modular IT Service Continuity Management Process that builds an end-to-end Service Continuity plan based on the Service Continuity plans of each component of the Services and integrating them with our Clients' Business Continuity Plans as required to meet specific requirements.

CGI Infrastructure used to provide this service is hosted within Tier 3 compliant CGI data centres. CGI data centres are constructed to an N+1 specification to provide mechanical and electrical infrastructure redundancy to mitigate against incidents, which may be caused by an interruption to power or cooling.

Operation of our data centres is covered by our IS27001 certification. CGI collaborates with specialist solution providers for Business Continuity and ITDR services. We contract for provision of temporary accommodation, in the unlikely event of a major disruption, which may be configured as either desk or data room space.

3. Onboarding and Offboarding

3.1. Onboarding

Our on-boarding planning approach commences with an in-depth requirement gathering exercise to capture your business objectives and security governance obligations fully. Subsequently, we adopt a methodical process to identify, prioritise, and rectify security vulnerabilities across your organisation's systems, networks, and applications.

Collaboratively, our Service Transition Team liaises with your stakeholders to validate the target infrastructure, categorising, and prioritising critical services, typically through asset lists and IP addresses, to ensure accurate alignment with security enhancement goals. The next step involves developing a remediation plan to address identified vulnerabilities. This plan outlines the steps, resources, and timeline required to remediate vulnerabilities effectively.

Routine remediation efforts will include applying patches on a monthly or quarterly basis (depending on requirements and vendor releases), implementing configuration changes, updating software versions, or deploying additional security controls. This structured methodology ensures that our efforts are tailored to meet the specific needs of each client.

3.2. Offboarding

Service Off-boarding is instigated by a client request or after expiration of the service agreement. Removal of tooling and supporting infrastructure and deletion of any 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.

Pricing of this service is dependent on requirements; please contact CGI for details. After client notification that data has been successfully recovered, CGI will purge and destroy client data from any compute or storage device/media that remains part of CGI's estate.

4. Service Constraints

Services are provided remotely from our operations centres in South Wales. Services require suitable communications links which can be arranged and co-ordinated at additional cost.

5. Service Levels

Full support of CGI services is provided as standard via the CGI Service Desk. The Service Desk is 24x7x365 and is resourced with 1st / 2nd line technical support engineers. Our service desk has direct escalation to 3rd line support and onward escalation to product vendors.

6. Technical requirements

Services are provided remotely from our operations centres in South Wales. Services require suitable communications links which can be arranged and co-ordinated at additional cost.

7. Security

As an experienced managed security services provider (MSSP), CGI provides clients with the expertise and capabilities required to implement and operate highly secure infrastructures, focusing on:

- Governance, risk, and compliance to increase regulatory compliance and reduce audit costs and findings.
- Risk management to protect information and critical assets and ensure confidentiality.
- Infrastructure protection management to deliver the latest security network and systems technologies.

We have invested heavily in establishing our credentials, working closely with international security associations and standards bodies.

Our approach to information security management and data protection is inherently built into our daily operations. All our staff will work continuously to maintain the security of data and services entrusted to us. This is a corner stone of our risk management approach. We base our operations on a standard set of policies and procedures. Where required, each programme will develop tailored, programme specific, procedures that will ensure the interface with client procedures is well integrated and understood.

We are delighted to confirm that:

- We comply with the International Standard for Information Security ISO/IEC 27001. Our data centre infrastructure services and several other services hold and maintain ISO/IEC 27001 certification.
- Our service complies with UK Government Security Classifications (GSC) to ensure that sensitive government information is appropriately protected, shared only with authorized personnel, and handled in accordance with security protocols.
- We comply with the Data Protection Act, CGI UK Limited is registered as a data controller under the Data Protection Act 1998, registration number Z6949379.
- Our service is audited to the following standards: ISO 9001(Quality), ISO 27001 (Security/Risk), ISO 14001 (Energy efficiency).

8. Service Pricing and Terms and Conditions

8.1. Pricing

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

8.2. Terms and Conditions

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

9. 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.

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

3. Your name and contact details.
 4. A brief description of your business situation.
 5. Your preferred timescales for starting the work.
- 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

