



Business Continuity as a Service (BCaaS)

Contracting body

30 Jan 2026

Issue 2.0

Table of contents

- 1. Service Description 5**
 - 1.1. Are you ready for a disaster? 5
 - 1.2. Overview of the continuity services 5
 - 1.3. Business Continuity Steps 6
 - 1.4. Governance Assurance Framework 6
- 2. Data Backup and Restore 7**
- 3. Service Continuity 7**
- 4. Onboarding and Offboarding 7**
 - 4.1. Onboarding 7
 - 4.2. Offboarding 7
- 5. Service Constraints 7**
- 6. Service Levels 8**
- 7. Hosting Options and Locations 8**
- 8. Security 8**
- 9. Service Pricing and Terms and Conditions 8**
 - 9.1. Pricing 8
 - 9.2. Terms and Conditions 8
- 10. Further information 9**
- PROPRIETARY AND CONFIDENTIAL 10**

Service Definition overview

Organisations today are driven by agile delivery timeframes and pressure to cut costs and increase efficiency, while managing the risk of events and incidents that can disrupt service delivery and outputs.

To continually meet the needs of your service users, your organisation must be able to continue operations through any event or incident, whether caused through technical, infrastructure or personnel issues. It is crucial that your organisation employs sound, tested continuity measures and has recovery options in place to meet these potential interruptions; this starts with understanding your organisation and the risks to your critical outputs. Organisations that fail to understand their risks leave themselves open to financial loss, reduction in competitive edge and reputational damage.

In order to appropriately protect critical information and services from loss or interruption, it is essential that a robust approach is taken to Business Continuity Management (BCM). This involves the development and operation of a Business Continuity Management System (BCMS) that helps ensure that resilience and recovery is a well planned and documented process, minimising the organisational impact arising from a Business Continuity event.

Where there is a lack of effective recovery mechanisms an organisation may not be able to meet all of its operational requirements. This can have a direct impact on:

- The continued viability of the organisation itself through financial and reputational damage, including fines and penalties as well as loss of revenue and recovery costs.
- The general public, including loss of government services and the potential for serious injury if a service is safety critical or safety related.

CGI's proven approach includes:

- Analysis of the business needs of critical services and identification of key information assets to enable the delivery of those services; in terms of ISO 22301, this includes the identification of the key time periods for, RTO and RPO (Maximum Tolerable Period of Disruption, Recovery Time Objective and Recovery Point Objective).
- Identification of a total asset model, comprising technology, people, infrastructure and business partners that crucially enable service delivery.
- Allocation of assets against a set of seven standardised disaster types to ensure a comprehensive and coherent recovery plans can be developed.
- Identification and selections of recovery strategies that match cost, recovery time and business risk appetite.
- Development of business continuity plans; IT disaster recovery plans; and crisis media management plans.
- Rehearsals (aka exercising) of plans including desk checking, team walk-throughs, technical tests and full multi-modal exercises.
- On-going continual improvement of recovery options and posture to enable business confidence to be maintained.

Without adequate preparation, unexpected events can severely disrupt the effectiveness of an organisation; CGI's comprehensive approach will ensure your organisation has identified the key services and risks, along with effective strategies for resilience and continuity that are documented and exercised so you're ready for the unexpected.

Why CGI?

For over 40 years, CGI has supported government and commercial clients in safeguarding critical services and delivering some of the most complex and business-critical technology programmes. Our Business Continuity as a Service builds on this strong heritage by strengthening organisational resilience, ensuring continuity of operations, and aligning seamlessly with our broader portfolio of cyber, risk, and operational resilience services.

CGI has deep in-house expertise in delivering business continuity leadership and managed resilience services for a diverse range of organisations, from highly sensitive government bodies and regulated industries to large commercial enterprises and technology-driven businesses, helping them prepare for, respond to, and recover from disruption with confidence.

1. Service Description

As one of the largest security practices in the UK our experience in Business Continuity and resilience is based on over 40-years of working as a trusted advisor with Government and commercial organisations.

CGI has invested heavily in capabilities and infrastructure to support the Public Sector work it undertakes. CGI has a dedicated Security Directorate who maintains our List X facilities, clearances, accredited infrastructure, interconnections with government networks and the certification of our corporate infrastructure against ISO/IEC 27001:2022 and ISO 22301:2019. Our security consultants are provided with accredited CGI infrastructure which allows them to process protectively marked material on behalf of our clients and managing our own infrastructure to the highest of standards give us valuable insight and experience that we can apply to improve our client's resilience and responsiveness.

Members of the CGI security team maintain a wide range of security qualifications and certifications, including those specifically tailored to the requirements of the UK Public Sector, this includes the standard range of information and cyber security qualifications but also includes ISO22301:2019 auditors and practitioners, as well as members holding the Certificate of the Business Continuity Institute (CBCI).

As a consequence of the above capabilities and experience we are providing a comprehensive set of Business Continuity and IT Disaster Recovery services among our offerings that can be tailored to your specific needs, and to reflect your commercial, technical and regulatory perspectives. As one of the leading providers of IT Business Consulting services in the UK, CGI is well placed to:

- Prepare Business Continuity Plans; can be delivered as a suite of 'mini plans' to improve usability across local business units / teams in line with your organisational structure and culture.
- Assure third party services. We perform assurance and continuity assessments of suppliers and third parties.
- Advise on appropriate technical controls including alerting, reporting and monitoring.
- Review and update business and continuity related procedures and processes.
- Validate the implementation of recovery and resilience measures.
- Implement systems and processes to provide evidence of compliance and application of due diligence.
- Facilitate training and awareness campaigns for all members to ensure they understand their responsibilities.
- Prepare and exercise Media Plans for effective communication during any incident.
- Continuously monitor systems processing time critical services through our SOC and CTI capabilities.

1.1. Are you ready for a disaster?

Our high-level review provides clients with a short set of Self-Assessment questions which will enable an organisation to determine if they are require additional help in order to achieve an appropriate level of continuity. The questions cover areas such as roles and responsibilities; readiness for physical, technical, operational, personnel and supply chain incidents; and the level of validation undertaken to prove the suitability of your response. CGI can simply advise and make recommendations based on your responses, or work with you to complete an assessment if you prefer.

1.2. Overview of the continuity services

All organisations will face Business Continuity events and incidents; these can be caused by any combination of a lack of availability of services, personnel, or infrastructure. Any organisation must therefore be well prepared to effectively manage the impact against outputs for a broad range of potential events and incidents, causing minimum disruption and maintaining services to the highest possible levels. To support you in achieving this, CGI offers a suite of business continuity services including:

- Business Impact Analysis and identification of critical time periods.
- Threat and vulnerability assessment to identify the main risks to your services.

- Identification of measures that could prevent / reduce the potential for a disaster occurring or could detect the incident at an early stage.
- Identification of mitigation measures that could enable the business to recover to an agreed level of operation in a timely manner.
- Development of recovery strategies that balances recovery time, risk appetite and costs.
- Development of a suite of business continuity and IT disaster recovery plans.
- Training of members, at all levels, in business continuity and their role(s) within it.
- Graduated series of rehearsals (exercises).

1.3. Business Continuity Steps

CGI strongly advises that businesses take appropriate steps to ensure they are prepared for a Business Continuity event or incident. Our recommendations include:

- Performing a Business Impact Analysis, in accordance with ISO22301:2019 and the Business Continuity Institute Good Practice Guide (GPG) - without it a business will not know its risk exposure.
- Review the technical, physical and personnel-based threats that could trigger a disaster.
- Identification of protection that could reduce the likelihood of an incident occurring and/or enable an incident to be detected in a timely manner; thus allowing mitigation to be put in place rapidly.
- Training of all members as to their personal roles in the event of a disaster; CGI recommends that this is carried out at three levels:
- Training for all members as general awareness and to help them recognise the supporting roles that they may have during recovery operations.
- Training for all individuals named within a continuity plan (either as the personnel responsible for certain actions, or as a deputy if the primary individual is not available at the time of a disaster).
- Training for those responsible for managing a specific area of recovery to ensure they fully understand their place in the overall recovery, as well as their potential authority to modify or update plans during recovery.
- Identify a "Business Continuity Manager" and ensure that the role is fully defined to enable the individual to successfully manage process, brief senior leadership and maintain and update relevant documentation.
- Deliver on-going rehearsals and exercise / tests for directors, managers and all members responsible for recovery of the business during a disaster.
- Audit any third parties' recovery posture to ensure that a disaster affecting them does not critically wound your business.
- Review contracts and agree who is responsible for what and who is implementing what level of resilience and recovery.

Our consultants have a proven track record in delivering recovery solutions and will be available to make a significant contribution in assisting organisations in making the necessary changes.

1.4. Governance Assurance Framework

CGI has an established and tested methodology for undertaking continuity assessments. This adapts an enterprise approach to the business continuity domain, and it leverages our extensive experience in undertaking security assessments for UK Government and CNI clients. ISO/IEC 27000, ISO 22301, ISF, COBIT and ITIL standards and frameworks are combined with national and local regulatory requirements and good practice guidance for the domain under analysis.

The reviews will be completed through a series of structured interviews, documentation review (policies, procedures and validation) and understanding relevant business capabilities and technical readiness. You will be involved and consulted at all stages of this process, that results in a comprehensive 'failure matrix' being produced that captures the key Business Continuity requirements and recommended solutions for your organisation, that forms the basis of your future strategy for Business Continuity and resilience.

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 2.0 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

