

Business Continuity Management Service G-Cloud 15





Table of Contents

1	Service Overview	3
2	Business Need	3
3	Our Approach.....	5
4	Buyer Responsibilities	6
5	Service Management	7
6	Protection of Data	7
7	On-boarding and Off-boarding	7
8	Skills and Knowledge Transfer	7
9	Vendor Accreditations/Awards	8
10	Sub-contractors	8
11	Business Continuity and Disaster Recovery	9
12	Pricing	9
13	Ordering and Invoicing	9
14	Termination Terms	9
15	Further Information	9



1 Service Overview

With increasing moves to digital and cloud enabled services, business continuity and disaster recovery are key services that all public sector organisations need to operate effectively. Ensuring that business operations and services are maintained for internal and external customers is fundamental for clients; but being so intimately connected with citizens and consumers also exposes organisations far more in terms of reputation in the event of failure of service and business continuity responsibilities. Increasing use of 3rd-parties also adds to the complexity and risk.

Business continuity is important in cloud services environments where clients may have one or more 3rd-parties delivering key services, and more operational security interfaces and channels to manage, operate and assure. It is important that cloud service providers have business continuity plans sufficient for your services and that your data is secure in the event of a service failure and recovery. It is also important that the interactions between your enterprise and cloud services are understood in terms of risk, and that business continuity plans exist that address the failure of one or more service elements.

Through our experience with our major public sector clients, Capgemini's business continuity consultants are experienced in developing and implementing business continuity solutions and services for clients, and our approach recognises that people, contracts and communication are just as important as information and IT.

Capgemini uses the framework provided by the BCI, that is, the Business Continuity Institute's 'Good Practice Guidelines' (GPG) - and ITIL. We also reference and use industry standards such as the HMG Security Policy Framework and ISO 22301.

Capgemini's business continuity consultants work with clients to deliver customised business continuity management plans and activities which are comprised of the following:

- Facilitating workshops and 'one-on-one' training;
- Conducting business impact assessments (BIA) and identifying critical time frames; for example, the maximum tolerable period of disruption (MTPD), recovery time objective (RTO) and recovery point objective (RPO). MTPD is the maximum acceptable length of time that can elapse before the lack of a business function severely impacts the organisation. RTO is the maximum agreed time for the resumption of the critical business functions. RPO is the point to which information must be restored to enable the activity to operate on resumption;
- Identifying and analysing in scope internal and external stakeholders and 3rd-parties;
- Identifying key dependencies between the enterprise and cloud environments;
- Performing risk assessments;
- Developing response and resumption strategies;
- Developing test plans and conducting tests based on realistic scenarios.

Our approach and public sector experience help clients manage their business risks, protect their reputation and ensure that their Third Parties deliver.

The business continuity management service provides business analysis, design, consultation, and service management in support of the design and implementation of cloud-based services.

This service can be provided onshore or offshore.

2 Business Need

Ensuring that business operations (people, processes, accommodation, suppliers and IT) continue to operate in the event of an incident, crisis or disaster is a fundamental client business requirement particularly in respect of sound risk assessment and financial planning.



Cloud and digital services adoption can provide clients with new business opportunities and the ability to reach more citizens or consumers. However, as more Third parties and channels may be involved in delivering services, there are more security interfaces and Third party risks to manage. Clients need to ensure that not only do their cloud providers and cloud applications have suitable business continuity plans for your services, but that data also remains secure during continuity and recovery processes.

Clients should also ensure that the technical and human interfaces between their enterprise and cloud services environments and applications are well understood in terms of risk and form part of their business continuity plan. These considerations often mean that clients require additional levels of expertise to plan and test business continuity for cloud services and applications.

The Business Continuity Institute's 'Good Practice Guidelines' (GPG) includes a framework that clients are recommended to consider based on industry experience, enabling continuity of a client's own operations. The ITIL framework also includes business continuity aspects under IT Service Continuity Management to guide clients. The impacts of Third parties are also important considerations of both frameworks. Capgemini consultants bring their experience in using these frameworks.

There are also several compliance frameworks that include business continuity as mandatory components:

ISO / IEC 27001 – which includes framework sections on security aspects of business continuity and Third parties. Organisations seeking ISO / IEC 27001 compliance or accreditation need to consider these aspects:

- Business continuity planning, control, implementation, verification, review and evaluation under ISO / IEC 27002 (5.29 Information security during disruption / 5.30 ICT readiness for business continuity)
- Supplier relationships under ISO / IEC 27002 (Section 5.22.k), where clients are required to ensure that suppliers maintain sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.
- HMG Security Policy Framework - Section 2.10 Preparing for and Responding to Security Incidents
 - This policy framework states:

"Government organisations will have:

- Business continuity arrangements aligned to industry standards, to maintain key business services, building resilience and security to facilitate a rapid and effective response to recover from incidents.
- Processes in place to regularly conduct risk and vulnerability assessments and review resilience planning for critical assets, particularly those identified as Critical National Infrastructure."
- BS EN ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements
- This International Standard specifies requirements for setting up and managing an effective Business Continuity Management System (BCMS).
- Providing assurance of Third parties is an essential part of the business need. Can you be sure that your Third parties will deliver their essential services in the event of incidents? What are their plans and are they fit for purpose? How dependant are your business processes on these? Involving Third parties in regular BCP communications and rehearsals is recommended to enable measurement of their performance. Confirming that contracts adequately cover business continuity risks in the event of failure of Third parties should also be assessed.
- Reputational management: business continuity includes business aspects such as protecting and management of reputation in the event of incidents, and communication with the press. These considerations are of high importance for organisations and include communication of responsibilities to the client's staff, and the Third parties involved.



Capgemini's consultants have experience in helping to manage all of these business needs.

Capgemini can support in many aspects of a business continuity programme. Some examples are:

- Business continuity management system (BCMS);
- Policy and programme management;
- Embedding business continuity – awareness and training programmes;
- Conducting business impact analysis (BIA);
- Business continuity planning;
- Gap analysis;
- Scenario testing;
- Training & workshops;
- Project management;
- 3rd party assurance and business continuity maturity;
- Resilience reviews using standardised process, tools and approach;
- Reputation management.

Capgemini can provide a range of Cyber Security services to enable clients to deliver business benefit through enhanced business continuity. Elements of this service can encompass security management, security strategy and transformation, governance risk and compliance, architecture design & implementation, identity and access management, cyber analytics and protective monitoring and education and awareness of security and business continuity.

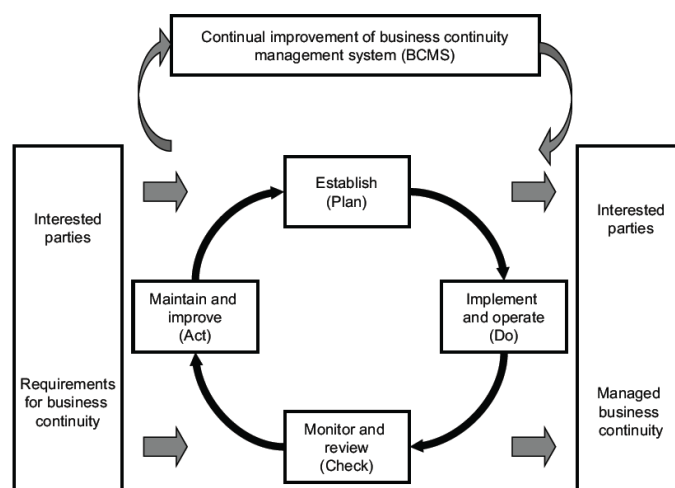
Capgemini has over 500 security professionals based in the UK whose expertise can be leveraged to provide our clients with cyber security services.

3 Our Approach

Through our experience with major public sector clients, cloud enablement and thorough understanding and use of standard frameworks, Capgemini is able to help clients design the best approach for their specific business needs.

This can include providing resources to help clients deliver their cloud services business continuity planning and testing; and working with the client's cloud services providers.

In consultation with key client staff and management, and using the frameworks provided by the Business Continuity Institute's 'Good Practice Guidelines' (GPG), ITIL, ISO / IEC 27001 and ISO22301 Capgemini can develop customised business continuity management solutions which address business functions and processes, IT system applications, key people and interested parties involved, key dependencies, Third parties and associated risks. Capgemini can help organisations verify that these processes are regularly reviewed and continue to operate through the ISO22301 Plan, Do, Check, Act process as illustrated in the following diagram:



This diagram is for illustration only and does not represent any obligation or responsibility of Capgemini.

Depending on the services purchased, Capgemini's Business Continuity services can assist clients to achieve benefits such as:

- A Business Continuity policy endorsed by the client's top management and communicated throughout the client's organisation;
- BC roles, responsibilities and competences defined and communicated;
- BC representatives in the client organisation educated about the principles, concepts, assumptions, methods and techniques to be applied;
- Improved understanding of the resilience of the client's business and operating model;
- Identification of key value-creating products and services;
- Identification of key dependencies – priority assets and processes;
- Planning how the client's organisation would respond to a loss or threat to any of these;
- A model for assessing the cost-benefit of recovery options;
- Capturing the main threats today and on the horizon;
- Providing evidence that the continuity plans will work in practice;
- Action plans to address issues identified by BC exercises;
- A Business Continuity Management System set up in line with the Business Continuity Institute's Good Practice Guidelines;
- A project plan to achieve certification against ISO/IEC 22301;
- A BC Audit Programme to provide assurance and a Continual Improvement Framework.

4 Buyer Responsibilities

Please refer to the Supplier Terms listed with this service on the Platform. These may contain additional Buyer obligations/costs the Buyer is subject to that are not identified anywhere else in the Supplier's Application or on the Platform.

The following Buyer responsibilities will apply:

- The Buyer will provide a project/engagement manager to act as a single point of contact and an escalation route for the full duration of the project/engagement;



- The Buyer will make available appropriate subject matter experts (business and technical) as appropriate to support the project or delivery plan;
- The Buyer will be responsible for providing detailed requirements by the mutually agreed date;
- The Buyer will progress the introduction of the service through any internal service introduction/gating process, Enterprise Architecture processes and any other standard processes that are necessary;
- All internal and external user communications will be managed by the Buyer;
- The Buyer will make any network changes to their networks as required for the project;
- Any changes to existing environments required for the service will be Buyer's responsibilities;
- The Buyer will also provide any required test environments and test data reflective of the target implementation environment(s).
- Depending on the service model chosen, the Buyer may have other responsibilities which will be discussed, agreed and then described in the Order Form.
- If these responsibilities do not match your expectations, then please contact us in order that we can explore options to vary our approach.

5 Service Management

Capgemini's service can be consumed in the following deployment and delivery models, all fully managed by Capgemini. Please contact us to discuss which of these fits your requirements. These are:

- **Offshore resources:** Our consultants work from our offshore locations. This provides a very cost-effective solution with access to a large pool of related skills.
- **Onshore resources:** Our consultants work from our UK offices. This provides a cost-effective solution for buyers that require UK delivery.
- **Dedicated resources:** Our consultants work on your sites, embedded as part of your team. This provides a solution for buyers that require skills augmentation and a high degree of control over the work.

6 Protection of Data

This service is based on a security classification of 'Official', however should you have a requirement for a different security classification that you would like us to consider, please contact us to discuss.

7 On-boarding and Off-boarding

Capgemini shall undertake on-boarding and off-boarding activities agreed within the Order Form (including as a minimum an exit plan in line with the Call-Off Contract terms) which will be charged for in accordance with the Pricing section for this service.

8 Skills and Knowledge Transfer

Capgemini recognises that skills and knowledge transfer is a critical element in the provision of G-Cloud services to public sector clients. Where possible and applicable, this forms part of the delivery plan for the service agreed at the start of the engagement. Our consultants and engineers are experienced in providing skills and knowledge transfer for major private and public sector clients.



Where appropriate, we may use a standard approach, tailored to topic, skills-gap and individual, to ensure consistency and effectiveness. The approach, Capgemini's Assess-Plan-Implement framework, has been used repeatedly by our teams to structure the work involved in transferring skills and creating new teams capable of driving and sustaining change long after the end of the formal programme. The framework can be applied throughout a project to understand knowledge transfer objectives, plan training delivery methods and materials, and deliver and evaluate success.

9 Vendor Accreditations/Awards



For the 13th year in a row, Capgemini has been recognised as one of the World's Most Ethical Companies® by the Ethisphere® Institute. This is an acknowledgement of our ethical culture that makes us an employer of choice and responsible player in the eyes of our clients, shareholders, and the wider community.

Capgemini can provide security delivery professionals with the following industry certifications:

- NIST Cybersecurity Framework (NCSF);
- Certified Information Privacy Professional/Europe (CIPP/E);
- Certified GDPR Practitioner;
- Certified ISO/IEC 27001 Lead Implementer;
- Certified ISO/IEC 27001 Lead Auditor;
- Certified Information Systems Security Professional (CISSP);
- Certified Cloud Security Professional (CCSP)
- Certificate of Cloud Security Knowledge (CCSK)
- Certified Information Security Manager (CISM);
- Certified Information Systems Auditor (CISA);
- Certified Ethical Hacker (CEH);
- TOGAF9, SABSA and other architectural methodologies including Capgemini's own;
- IT security specific MSc or PhD;
- Membership of the Chartered Institute of Information Security Professionals (CIISec)
- Certified in Risk and Information Systems Control (CRIS)
- Computer Hacking Forensics Investigator (CHFI)
- Capgemini delivery staff hold a wide range of vendor specific certifications for many types of cybersecurity tooling.

10 Sub-contractors

Capgemini can offer these services using either onshore UK resources or offshore resources. Should the Customer choose an offshore service from India, then Capgemini UK may use the following subcontractors to deliver this service:

- Capgemini Technology Services India Limited.



11 Business Continuity and Disaster Recovery

No disaster recovery plan is provided as part of these Services.

12 Pricing

This service is priced in accordance with the SFIA Rate Card attached. Capgemini can also provide offshore resources at reduced rates where appropriate. Projects can be priced either on a Time & Materials or Fixed Price basis.

13 Ordering and Invoicing

Please refer to the Supplier Terms for this service.

We would be pleased to arrange a call or meeting to discuss your requirements of our service in more detail.

14 Termination Terms

Please refer to the Supplier Terms for this service.

15 Further Information

For more information about this or any of our G-Cloud services, please contact our Public Sector Team.

Phone: 0370 904 4858

Email: publicsector.opps.uk@capgemini.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.

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Make it real. | www.capgemini.com



This presentation contains information that may be privileged or confidential and is the property of the Capgemini Group.

Copyright © 2026 Capgemini. All rights reserved.