

Cybersecurity – Secure by Design (SbD) - Assessment Service G-Cloud 15





Table of Contents

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



1 Service Overview

The Secure by Design (SbD) approach is the new Government cybersecurity assurance approach that emphasizes integrating security measures into the very foundation of digital systems and products. Assurance is undertaken from the outset, supporting ongoing continuous maintenance, review and revision of controls in relation to changing business needs, risks and threats.

Capgemini's service offering helps Government and Industry understand the SbD Principles and the processes followed to enable them to meet and demonstrate SbD assurance (both within Central Government and MOD variants) of their Enterprise, Digital and Cloud enabled systems and services.

Capgemini's service can help Government and Industry by undertaking SbD assessments. It can also support our customers own SbD assurance processes by using the SbD Principles as a framework to help customers work towards effective compliance and assurance.

Although the outline aims and intents of SbD processes across UK Government adhere to the same intent, there are subtle differences in the approach and Principles used between the Central Government and MOD variants. These Principles are shown below:

Secure by Design Principles	
Central Government Variant	MOD Variant
1. Create responsibility for cyber security risk	1. Understand and define the context
2. Source secure technology products	2. Plan the security activities
3. Adopt a risk-driven approach	3. Implement continuous risk management
4. Design usable security controls	4. Define the security controls
5. Build in detect and respond security	5. Engage and manage the supply chain
6. Design flexible architectures	6. Assure, verify and test
7. Minimise the attack surface	7. Enable through life management
8. Defend in depth	
9. Embed continuous assurance	
10. Make changes securely	

Previous Experience

Capgemini undertook a pathfinder programme to assure a digital managed systems and services environment for the MOD at OFFICIAL SENSITIVE and above prior to the release of SbD. This allowed Capgemini to create an approach to the MOD SbD assurance process, through direct access to the programme.

In addition, Capgemini contributed to the Cabinet Office SbD programme and development of the SbD process through direct engagement and review by a senior level Cybersecurity Consultant.

These engagements have enabled us to contribute to lessons learned, central collateral and methodology development. Capgemini have taken these approaches forward and have undertaken/are undertaking SbD assurance consultancy and delivery for key strategic programmes and discrete projects for Government customers.

2 Business Need

SbD is a crucial approach that emphasises integrating security considerations into the very fabric of a system or service from its inception. The key benefits realised from this are:

1. **Early Risk and Threat Identification:** By adopting a SbD approach, organisations can identify security risks and threats during the initial stages of ideation and development and align appropriate controls. This proactive risk management approach allows security assurance requirements and vulnerabilities to be identified and addressed at the outset, and the identified controls to be incorporated into the design moving forwards. This also supports an adaptive approach to risk and threat management through life for the systems or services assured under SbD.
2. **Alignment with Business Goals:** SbD ensures that security aligns with the organisation's business case, mission and objectives rather than merely implementing what a standard requires. It focuses on what the business needs to achieve while maintaining robust security measures
3. **User-Centric Security:** Understanding user behaviours and their needs is essential. By working backward from user requirements, security can be designed to be suitable and usable for them. Continually reviewing user needs against security decisions helps strike the right balance between usability and security.
4. **Reduced Costs:** Considering security during the early stages of service development helps with reducing costs by avoiding expensive retrofits or rework later in the process.

In summary, SbD not only enhances security but also contributes to the overall success of digital services by ensuring they are secure, fit for purpose and adaptable to new requirements.

3 Our Approach

Our consultative approach encompasses the SbD assurance process incorporating NIST 800-37 (Rev 2). The high-level diagram below provides an indication of a typical SbD assurance implementation approach. Capgemini will work with customers to tailor this to their specific needs whilst retaining and adhering to the relevant SbD principles for the customer type (Central Government or MOD)



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



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 Buyer responsibilities as part of this service are as follows:

- The Buyer will define the scope of the area to be assessed.
- The Buyer will provide any training and awareness education to the security assessor as is required by the on-boarding requirements.
- The Buyer will provide a project manager to act as a single point of contact and an escalation route for the full duration of the project.
- The Buyer will make available appropriate subject matter experts and documentation (business and technical) to the project as appropriate to support the security assurance assessments.
- The Buyer will be responsible for providing detailed requirements by the mutually agreed date.
- The Buyer will announce the assessment to all appropriate individuals, asset and process owners.
- All internal and external user communications will be managed by the Buyer.
- The Buyer will accept the security assurance assessments report via post assessment presentation and be responsible for managing the recommendation identified from the assessments activity.

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:

- **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 assurance service is based on a security classification of 'OFFICIAL SENSITIVE' with BPSS/SC cleared resources.

Other classifications can also be assured, subject to discussion and agreement. 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 (CRISC)
- 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 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. 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.