

Cybersecurity Architecture Assurance Service G-Cloud 15





Table of Contents

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

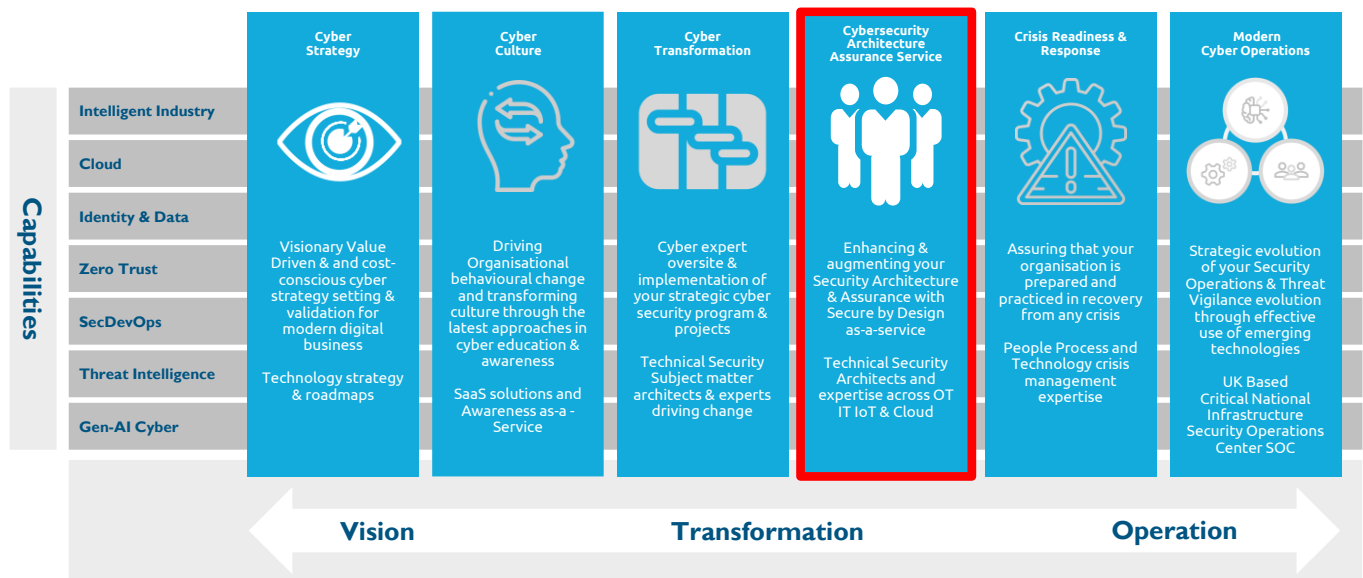


1 Service Overview

Capgemini Cybersecurity Architecture Assurance Service (CAAS) augments and accelerates the Chief Information Security Officer (CISO) and Security Programme objectives of protecting the enterprise and the need for organisations to ensure that information security is integrated into projects. This service embeds secure by design process and best practice in Procurement, Project Management, Solution Design and Project Delivery.

Capgemini CAAS provides skilled cybersecurity specialist Security Architecture and Assurance professionals to accelerate secure by design enterprise and cloud transformation programmes and projects. These valuable and in demand skills and approaches can be procured through flexible service models to accommodate your immediate, medium- and long-term requirements and strategy.

Capgemini CAAS standardises Security Architecture and Assurance and promotes Secure by Design principles on all cloud and technology transformation programmes and projects, addresses recruitment and skill development challenges and effectively demonstrates compliance with regulatory and audit requirements.



Cybersecurity Architecture Assurance Services (CAAS) focuses on enhancing and supporting security architecture and assurance across Operational Technology (OT), Information Technology (IT), Internet of Things(IoT) and Cloud environments. It ensures that cybersecurity is embedded from the start of technology transformation programs. CAAS provides expert guidance, technical security architects, and structured frameworks to help government organisations meet compliance requirements, strengthen resilience, and align with industry standards.

2 Business Need

The rapid move to cloud has increased cyber security workloads and created demands for new skills and approaches. Recruiting and retaining highly skilled cyber security professionals remains a challenge for many public sector organisations and arms-length bodies.

Legal and regulatory requirements are evolving continuously, and these organisations must provide more evidence of security and data protection practices. Cloud transformation programmes add complexity and expand the skillset for enterprise security architecture and assurance functions.

Fast adoption of cloud services can lead to misconfigured or poorly designed solutions, exposing sensitive government data, citizen personal information or public data. These vulnerabilities are actively targeted by cyber criminals and state-sponsored attackers. Threat actors are using advanced tools, including AI-driven techniques, to automate and refine attacks. Defenses must evolve as just quickly, requiring string strategies, processes and skills.



Managing cyber security risks in this environment requires a coordinated approach across leadership, technology, people and processes. Collaboration between public sector bodies, suppliers, and industry partners is essential to meet compliance obligations and protect critical services.

Capgemini CAAS helps Chief Information Security Officers (CISOs) and key stakeholders implement effective security architecture and assurance, manage project-specific risks, embed Secure by Design principles in all cloud and technology programs, address skills gaps, and demonstrate compliance with regulatory and legislative requirements.

3 Our Approach

The Cybersecurity Architecture Assurance Service utilises Capgemini's Project Cyber Risk Management (PCRM) methodology. This embeds a standard Secure 'By Design' approach in all projects and is aligned to the latest *ISO 27002:2022* International Security standard, specifically *Control 5.8 – Information Security in Project Management*. The PCRM methodology takes the following high-level approach:



1. **Context Review:** Understand the business objectives, project objective, high level plan and approach.
2. **Solution & Approach Review:** Understand the project's service/solution and data architecture, solution components and implementation plan, roles and responsibilities.
3. **Risk Assessment:** Assess the project/service/solution Cyber and Data Protection compliance risk against an appropriate or client preferred security framework e.g., NISR, ISO27001:2022, Organisational Security policy, Organisation Security Architecture standards etc.
4. **Risk Mitigation Plan:** Manage the risk by defining appropriate cyber controls, processes and ownership within the project and assigning ownership to these risks with the project manager.
5. **Risk Tracking & Reporting:** Monitor and report on the effectiveness of these controls via project risk register and established project management process and communications.

The CAAS team collaborate with key cloud security transformation stakeholders including security and technology leadership teams, project management and PMO, product and portfolio owners, solution architecture and service delivery to ensure buy in, awareness and alignment with secure by design philosophy, practice and processes.

While for many public service organisations onshore resourcing may be appropriate, we can also provide near-shore and off-shore resources for this service wherever possible.

This approach helps to provide the following:



- Supports ISO 27001, SPF compliance & accreditation activities.
- The CAAS team can call on wider Capgemini cloud and security community for support.
- Supports other stakeholders e.g. Information Governance, DR/BC, Caldicott Guardians.
- Can quickly adapt to meet changing threats and business requirements.
- Provides clear well-defined point of contact and subject matter steer for Project Security Architecture and Assurance matters.
- Supports implementation of NCSC guidance.
- Provides security professionals who are professionally qualified, e.g. CISSP, CISM, CISA, TOGAF9, ITIL, SABSA.
- Manages risks associated with Cloud use, third parties and Integrated Enterprise Portal (IEP).
- Helps address legal requirements for chain of responsibility in Personal Identifiable Information (PII) management.

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 provide details of existing PMO Project Management Office process, ownerships and accountabilities.
- The Buyer will provide details of any existing Enterprise Architecture process, ownership and accountabilities.
- The Buyer will provide details of any strategic/priority transformation programs to support demand planning and skillset planning activities.
- The Buyer will provide any existing organisation Security policy & Security Architecture standards.
- The Buyer will provide details of any existing Project Security Architecture process, ownerships and accountabilities.
- 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) and business owners as appropriate to support the CAAS team in their objectives.
- 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 regarding the CAAS service will be managed by the Buyer.
- Any changes to existing environments required for the service will be Buyer's responsibilities.
- 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 Capgemini to discuss which of these fits Buyer's requirements. These are:

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

6 Protection of Data

This service is based on a security classification of 'Official', however you should 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 Partnerships/Alliances

10 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.



ISO 9001 Quality Management for Management Consultancy and IT Implementation and services to the Public Sector



ISO 27001:2013 - Provision (Delivery) of IT services including business applications development, maintenance and Data, Digital and Cloud technologies.



NelsonHall has identified Capgemini as a Leader in its 2022 NEAT Vendor Evaluation for Learning Services due to its ability to meet future client requirements as well as its capability to deliver immediate learning benefits to them.



Capgemini is the first amongst consultancy and technology firms to be recognized six times in a row for its thought leadership reports.



2023 Ecovadis Platinum Rating: We maintained a platinum rating, recognising us as a responsible and sustainable business in the top 1% of companies assessed.



Better Society Awards: Our collaboration with Code Your Future to offer digital skills training won a Better Society Award in 2022. The awards celebrate efforts by commercial organisations to create a better society.



Inclusive Top 50 UK Employers List: We achieved second place in the Inclusive Top 50 UK Employers List 2022/23 – a list that assesses companies for best practice on diversity, equality and inclusion



UK Best Workplaces for Women: We were listed as a Best Workplace for Women by Great Place to Work®. This listing is based on responses from our team to an anonymous survey about their employee experience.



UK Best Workplaces for Wellbeing : We are listed by Great Place to Work® as a Best Workplace for Wellbeing



Great Place to Work: We were certified as a Great Place to Work® in 2023, reflecting our employees' experience of working at Capgemini in the UK.

11 Sub-contractors

Capgemini UK may use the following subcontractors to deliver this service:

- Capgemini Technology Services India Limited.



12 Business Continuity and Disaster Recovery

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

13 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.

14 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.

15 Termination Terms

Please refer to the Supplier Terms for this service.

16 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.