

# Security Consultant Service G-Cloud 14

November 2024





# Table of Contents

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



# 1 Service Overview

Capgemini can provide security consultants, ranging from Junior Security Consultant through to Principal Security Consultant, who can help to shape clients' information security designs by providing specialist security advice and guidance.

Capgemini's security consultants can provide advisory services to help clients devise, assess and, where appropriate, improve security strategies, security architectures, security management systems and information assurance (IA) arrangements for business systems or services be they hosted on client premises, in the cloud or as part of a hybrid model. Capgemini's consultants' have capabilities in risk assessment methods, risk management techniques, security maturity and compliance maturity assessments and the implementation and audit of Information Security Management Systems (ISMS).

Capgemini's security consultants have experience with cloud delivery, security and deployment models for IaaS, PaaS and SaaS and the up-and-coming Account – System – Server – Services hierarchy (AssS) service offerings provided by Amazon Web Services (AWS) and Microsoft Azure platforms. In each of these deployment models, clients may have one or more third parties delivering key services, and a mix of operational security interfaces to manage, operate and assure. Capgemini's security consultants have the capability to help clients understand and manage the security risks that accompany this complexity.

Capgemini's security consultants can be deployed in trusted client-side advisory roles, undertaking work once conducted under the auspices of the NCSC Certified Cyber Professional (CCP) scheme, or as an ISO 27001 Certified Lead Auditor or Lead Implementer. Capgemini's security consultants have experience in interpreting and applying the Security Policy Framework (SPF), Government Functional Standard GovS 007: Security requirements, GovAssure and the NCSC Cyber Assessment Framework (CAF), alongside advice and guidance from the National Technical Authorities, NCSC and NPSA. Capgemini's security consultants also have experience helping clients address legislative and regulatory requirements such as the General Data Protection Regulation (GDPR) and other data privacy concerns.

At the most senior level, Capgemini's Principal Security Consultants contribute to internal and external knowledge development internationally and operate at CxO level in major client organizations. They have experience of consulting in different business sectors, knowledge about different technical security solutions and the experience to identify and conceptualize new offers.

Managing Security Consultants and Senior Security Consultants are recognized security specialists who have experience of working in one or more business sectors and knowledge of security tools or technical security solutions. They have professional qualifications that confirm their experience and can deliver quality security consulting engagements including leading teams and liaising with clients' partners and vendors.

Junior Security Consultants and Security Consultants typically operate as part of a larger team. They can interpret and apply security-relevant management standards such as ISO 27001, the Information Security Forums' Standard of Good Practice for Information Security and the IT Infrastructure Library (ITIL). They can also deliver standards-based assessments.

This service supports Cloud based projects and services.

## 2 Business Need

Adopting cloud and digital services can provide clients with new business opportunities and the ability to reach more customers. Delivering these services can involve more third parties and channels, more security interfaces and more cyber security risk to manage. Often, clients need additional security knowledge to safely enable, manage, operate and assure their cloud and other digital services.

Capgemini's security consultants can respond to a wide range of business needs comprising security architecture design, transformational change, cloud adoption, risk assessment, ISO27001 gap analysis, proportionate security accreditation (including the production and maintenance of Risk Management Accreditation Document Sets where this is appropriate), General Data Protection Regulation (GDPR) and Network and Information Security (NIS) Directive, in CNI sectors, compliance, maturity assessments, security operations, digital forensics, incident management and fraud protection.

Capgemini's security consultants have capability to address business requirements ranging from low-level standards-based assessments through to executive level thought leadership and transformation.



## 3 Our Approach

Capgemini's Cyber Security Unit comprises over 500 full-time security professionals in the UK. These professionals routinely work alongside colleagues delivering broader consulting, technology, outsourcing and professional services, giving them a customer-centric view of security. Capgemini is a corporate member and supporter of industry bodies such as the Chartered Institute of Information Security (CII Sec), the Information Security Forum (ISF) and the International Association of Privacy Professionals (IAPP), as well as having members belonging to the UK Cyber Security Council and delivers a range of security services to major organizations in the public and private sector.

Capgemini encourages its security professionals to work collaboratively and flexibly, to think creatively and perform effectively. Through experience Capgemini has learnt how to leverage the methodologies used to enable information security consultancy services. Capgemini can deliver products and outcomes with spin-off benefits. Capgemini's approach is transparent making it straightforward for clients to understand what Capgemini's security consultants will deliver, when, and who else needs to be involved in the delivery.

Capgemini's Security Transformation Roadmap methodology combines information security, security architecture and enterprise architecture methods and reference models with programme management disciplines to define a coherent programme of work to transform security. Standards and guidance sourced from – for example – the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM), ISO/IEC 27000 series, NIST, ITIL publications, Information Assurance Standards, Good Practice Guides' (GPG) and NCSC Architectural Patterns, advice, and guidance, which can underpin the approach.

Capgemini Security Consultants can also draw on their experience of The Open Group Architecture Framework (TOGAF) or the Sherwood Applied Business Security Architecture (SABSA) to work with clients to devise, analyse and visualise security strategies and management systems across organisations.

## 4 Buyer Responsibilities

Please refer to the Supplier Terms listed with this service on the Digital Marketplace.

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;
- 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 and 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 recognizes 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 12th year in a row, Capgemini has been recognized as one of the World's Most Ethical Companies® by the Ethisphere® Institute. This is an acknowledgment 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](mailto: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, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the Future You Want | [www.capgemini.com](https://www.capgemini.com)



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

**Public** Copyright © 2024 Capgemini. All rights reserved.