Capgemini

Cybersecurity – Security Management – Run Service

G-Cloud 14

November 2024

Table of Contents

1 Service Overview

Capgemini can provide skilled cybersecurity professionals to help to shape your information security by providing specialist advice and governance for enterprise and cloud environments. Our Security Managers are experienced with HMG NCSC guidance, ISO 27001, NIS(2), DORA and the GDPR , for most types of run environments.

The general strategy in most situations is to detect and resolve issues at the earliest stage where this will have the least impact on delivery schedules or operational effectiveness.

2 Business Need

Security is increasingly complex and subtle. The threats against organisations and their information have never been higher. In addition, legal and regulatory requirements have been increasing significantly (e.g. DORA, GDPR).

At the same time, business and mobile applications are pervasive, being cloud based and citizen focused.

Failure to properly manage security throughout the application lifecycle can lead to:

- Lack of "secure by design" leading to increased risk and inadequate security in applications and systems;
- Lax development or operational activities due to poor oversight and review;
- Absent or poor reporting hindering governance and preventing management oversight;
- Poor governance and hygiene overall;
- Loss of control over third parties e.g. IEP and cloud providers;
- Easily avoidable security breaches – which may also keep recurring.

Some security breaches happen accidentally without malicious intent and in many cases the personnel involved have taken poor security decisions on their own. While the presence of a Security Manager is not a guarantee that such situations will not occur, it does significantly reduce the risk of this occurring and provide for a robust, consistent and effective response to incidents, which is imperative when personal information is involved.

Of course malicious attacks are growing massively and criminal hacking has become a major well-run and dynamic business in its own right. These attackers may target information which seems of little value to the business as they may be playing a longer game (e.g. harvesting intelligence for phishing or targeted attacks). A Security Manager will track the changes in the threat landscape and how these apply to your organisation.

The sustained surge in security incidents and events has also led to a massive demand for security professionals world-wide. This means that recruiting Security Managers can be problematic especially at short notice or for part-time engagements. Capgemini's security teams are mutualised and in place which gives a level of flexibility direct recruitment cannot provide.

3 Our Approach

Capgemini Security Managers will take responsibility for the security matters agreed under this service. This can consist of the following:

- The overall security situation of the system in scope is monitored and appropriate actions are taken to maintain this;
- Effective coordination with security stakeholders (e.g. Assessors , ESA, Caldicott Guardians, DR/BC) and business owners;

- Security issues are recorded in a risk register, mitigations etc. are discussed and approved by risk owners and remediation is monitored and reported on;
- Assurance activities such as penetration testing or audits (including site visits) are arranged as necessary;
- Compliance of third parties (e.g. cloud providers, sub-contractors, information exchange partners (IEP)) with security policies etc. is monitored, and actions are taken to maintain compliance;
- Change control requests are analysed for security impact and recommendations etc. are made accordingly;
- Any project teams operate themselves in an appropriately secure and integral manner, in the standard environments (development, testing, pre-production etc.) to maintain the security of the run environment;
- Architecture and design appropriately address external (e.g. legal) and internal (e.g. HMG or local policy) security requirements;
- Act as a central point of contact for all security matters;
- Provide considered security advice, threat assessment and security awareness as required;
- Support accreditation, project gate, service introduction and similar activities;
- Undertake periodic assurance activities to ensure the implemented control set is functioning as intended
- Drive CSIP activities to improve controls, especially as a result of an incident
- Create and maintain security documentation as appropriate and participate in review of material such as policies and procedures;
- Act as custodians for sensitive assets;
- Respond to security events (including DR as well as security incidents) as required, and be involved in their planning (if needed);
- In general act as a trusted extension of the organisation's security and compliance teams;
- Call in specialist security team members for advice or services as required;
- Oversee the secure decommissioning of systems or disposal of media;
- Report regularly to stakeholders.

Capgemini provide our Security Managers from dedicated or mutualised teams. We can provide the service part-time or full-time, during normal business hours .

Using mutualised teams means that service can be maintained in the event of sickness or holidays, and it also makes available a wider pool of security knowledge and experience. We also have managers with specific certifications or experience.

While for many HMG organisations on-shore resourcing will be appropriate, we can also provide near-shore and off-shore locations for this service.

This approach helps to provide the following:

- Supports ISO 27001, SPF compliance & accreditation activities;
- Managers 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 for security matters and incidents;
- Supports implementation of NCSC guidance;
- Provides Security Managers professionally qualified, e.g. CCP, CISSP, CISM, CISA, TOGAF9, ITIL, SABSA, CRISC, ISO27K LA;

- Can manage risks associated with cloud use, third parties and IEP;
- Helps address DPA requirement for chain of responsibility in 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 following client responsibilities will apply:

- The client 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 client will make available appropriate subject matter experts (business and technical) as appropriate to support the project or delivery plan;
- The client will be responsible for providing detailed requirements by the mutually agreed date;
- The client 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 client;
- The client will make any network changes to their networks as required for the project;
- Any changes to existing environments required for the service will be client's responsibilities;
- The client 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. Additional requirements this may be subject to additional Charges in accordance with the SFIA Rate Card.

7 On-boarding and Off-boarding

Capgemini can 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 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 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

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