Capgemini

Information Risk Management Lifecycle Service

G-Cloud 15

Table of Contents

1 Service Overview

Capgemini's Security Practice can support different areas of Information Risk Management activities in accordance with policies, standards, and guidance used by HM Government and industry:

Security Policy Framework (SPF);

- Government Functional Standard GovS 007: Security;
- GovAssure;
- HMG Information Risk Management Guidance, such as NCSC and NPSA risk management approaches;

Legislative and Regulatory frameworks, such as, the Data Protection Act/ General Data Protection Regulation (GDPR) and the Network and Information Systems (NIS) Regulations;

- ISO27001 family of Standards, including ISO27005 – Information Security Risk Management;
- Information Security Forum (ISF) - The Standard of Good Practice for Information Security;
- ISF Information Risk Analysis Methodology (IRAM) and Quantitative Information Risk Assessment (QIRA) Methodology.
- Secure by Design - creating a dynamic risk management process that will respond to emerging threats
- Cyber Resilience - support of, and guidance for, resilience initiatives

Capgemini's Security Information Risk Advisors can provide business driven and method-based advice on the management of security and information risk. This can explain to risk owners and other stakeholders the causes, likelihood, and potential business impacts of information risks throughout the information system lifecycle.

Cyber Security information risk management is important in hybridised enterprise/cloud services environments where clients have one or more third party providers of integrated enterprise and cloud services, resulting in complex operational security interfaces and channels to manage, operate and assure.

Our Security Information Risk Advisors can take responsibility for managing agreed information assurance (IA) and accreditation activities to provide business driven advice on the management of security and information risk consistent with Industry and HMG IA policy to act as a business enabler and facilitate good information governance. Our Security Information Risk Advisors can also support Information Asset Owner's (IAOs) in their duties to understand and address risks to their assets and help provide the required assurance to senior board level risk owners.

The level of engagement depends upon the project scope, but typically covers:

- Identification of critical information assets that require protection;
- Support for production of impact assessments, including Privacy Impact Assessments (PIA);
- Being a focal point for escalation and resolution of security/information risks;
- Reviewing architecture artefacts to identify, analyse, and evaluate information risks that arise from proposed solution architectures and threats to assets;
- Reviewing externally produced vulnerability assessment reports and expressing risks in a business context;
- Developing security risk assessments using applicable and proportionate methodologies in accordance with HMG IA and industry guidance. Our SIRA are experienced in HMG risk assessment methodologies and producing gap analysis using appropriate controls such as ISO27001 which focus attention on policies, processes and procedures to support risk assessment;
- Developing information security and risk management strategies to reduce risk, and present options for informed and effective risk treatment decisions by risk owners;
- Developing security risk assessments to inform and support an organisation's formal assurance requirements;

- Supporting and promoting security and privacy awareness;
- Supporting the design and implementation of Cloud based projects and services.
- Supporting compliance and assurance activities

2 Business Need

The Information Risk Management approach that Government Departments and Agencies are advised to follow is designed to ensure that an organisation assesses and makes appropriate business decisions about its technologies and information risks. HMG Cyber Security Strategy sets out that organisations must become cyber resilient, to ensure they can continue to deliver the functions and services which maintain and promote the UK's economy and society.

This requires a Department or Agency to develop an IA governance framework with a risk management strategy that helps an organisation protect itself, and which provides confidence that the technology and information used is secure enough to meet its needs. Cloud and digital services adoption can provide Buyers with new business opportunities and the ability to reach more users, citizens, and consumers. However, increased integration of third party provided enterprise and cloud services results in more security interfaces and third-party risks to manage. Furthermore, the needs of an organisation, the threats it faces, and the vulnerability of its technologies and information is constantly changing. This often means additional levels of security expertise are required by Buyers to enable, manage, operate and assure these services.

Information risk management needs to be embedded throughout the technology lifecycle of a system or service, informed by a realistic view of risk and a clear understanding of the organisation and its objectives. Capgemini's Security Information Risk Advisors are experienced in providing advice on different areas of Information Risk Management activities, in accordance with policies, standards and guidance determined by HMG, industry and increasingly legislative and regulatory requirements.

Capgemini's services can be procured as stand-alone elements, or to provide an end-to-end risk management process for identifying and managing technology and information risks. For example:

- Implementing strategies to drive information risk management within an organisation to enable informed decision making by Business Leaders;
- Developing risk assessments, based on National Technical Authority (NCSC and NPSA) guidance, as well as utilising legacy approaches, including those based on HMG IS1/2 where still in use;
- Deploying proportionate and cost-effective risk management approaches if formal assurance is not required. Capgemini can provide risk assessment services to manage technology and information risks against specific assets that require protection – delivered using either agile or waterfall approaches;
- Through-life risk management which can also play a significant part in an organisation's ability to support its legislative and/or regulatory compliance, such as, the Data Protection Act/ General Data Protection Regulation (GDPR) and the Network and Information Systems (NIS) Regulations;
- Supply Chain Assurance which is now a mandatory requirement across Public Sector clients and their suppliers (and some Private Sector clients), to assure the security risks within their supply chain. This can include cloud services providers.
- Capgemini's approach to security assurance which can help promote the adoption of consistent security controls that can protect the Buyer's business operations against the potential for poor practices, both physical and procedural, that could result in:
    - The theft or loss of the Buyer's physical or information assets;
    - Damage to such assets which causes disruption to the Buyer's operational capabilities or otherwise discredits the Buyer or damages the Buyer's reputation;
    - Malicious changes to software products, such as the corruption of data or the introduction of unauthorised components to hardware assets;

- The potential for security complacency through failures to promote effective security training and awareness within the workforce.

3 Our Approach

Capgemini's Security Information Risk Advisors have access to a vast array of resources that enables them to work with Buyers, and depending on the service purchased:

- Advise on information risk management needs and approaches to a Buyer's needs, to embed information risk management;
- Assess third party and cloud services against an agreed scope;
- Communicate information and technology risks to support an effective risk decision-making culture where security risks are considered and integrated;
- Maintain the Confidentiality, Integrity, and Availability of the Buyer's business systems and associated data through appropriate risk identification and treatment;
- Maintain the Availability, Integrity and Safety of the Buyer's Operational Technology (OT) systems through appropriate risk identification and treatment;
- Help make sure that technology and information risks are documented, owned, and treated;
- Demonstrate that Buyers' systems are compliant with Government Functional Standard GovS 007: Security and meet the desired outcomes from the Security Policy Framework.
- Security assurance and compliance activities can be tailored to the specific needs of the Buyer but can consist of any of the following:
- ISO27001 assessments as a precursor to audit by an approved certification body;
- Physical security and procedural assessments structured around either ISO27001 standard or NPSA Protective Security;
- Further security and procedural assessments of hybridised Enterprise/Cloud environments against ISO27017 and ISO27018 standards where required;
- Review of compliance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679);
- National Protective Security Authority (NPSA) Operational Requirements (OR) Level 1 & 2 assessments;

The approach can help deliver the following benefits:

- A coherent, risk-based security assurance strategy;
- Assurance that practices are consistent with the Buyer's security policies;
- Identification and resolution of security vulnerabilities;
- The provision of cost-effective solutions, where security enhancements are necessary;
- A reduction in the number or likelihood of security incidents and related mitigation costs;
- A scalable solution, tailored to address simple to complex supply chain models;
- Security controls that are in line with the Buyer's stated needs and expectations;
- Confidence that physical and procedural security measures are commensurate with the logical security controls designed into the Buyer's business systems;
- Reassurance that security controls are designed around HMG and industry standards and good practices;

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**: Capgemini consultants work from Capgemini offshore locations. This provides a very cost-effective solution with access to a large pool of related skills.
- **Onshore resources:** Capgemini consultants work from Capgemini UK offices. This provides a cost-effective solution for buyers that require UK delivery.
- **Dedicated resources:** Capgemini consultants work on Buyers sites, embedded as part of Buyers 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 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 individuals, 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.
- PCI DSS Qualified Security Assessors (QSA)

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