Capgemini

Enterprise Security Projects and Consulting (ESP&C) Service

G-Cloud 15

Table of Contents

1 Service Overview

Capgemini's Enterprise Security Projects and Consulting (ESP&C) service provides services to help clients devise, assess and, where appropriate, improve security strategies, security architectures, security management systems, information assurance (IA) arrangements, and security solutions 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, enterprise architecture frameworks and the implementation and audit of Information Security Management Systems (ISMS). In addition to the advisory elements, our ESP&C can also provide buyers with security solution (technology and process) design and build capabilities.

Enterprise security architecture provides a framework for building and operating secure systems and secure enterprises and sits at the core of our approach to enterprise security services. It can help enable clients to determine the appropriate amount of security – enough to meet the applicable threats and regulatory requirements, but not so much as to be excessively costly or to erect unnecessary barriers to transformation. It can help clients who want their systems to be 'Secure by Design' through derivation of artifacts that display the traceability and support of through-life secure operation of services required by SbD. 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. Capgemini also provided expertise into the Cabinet Office Industry Panel relating to Secure by Design.

A common thread across our ESP&C services is identifying, describing, and prioritizing risks and then identifying and developing the appropriate security controls in a traceable manner – essentially enabling the organisation to answer the question of "why" with respect to security measures. This traceability is especially important when clients are adopting cloud services and environments which may have one or more third party providers of integrated enterprise and cloud services; clients need consistent and cohesive security throughout their wider supplier ecosystem, alongside full clarity of delivery responsibility for the security of services and data. Capgemini can help clients by providing security architects experienced in deriving appropriate security governance structures, architecture frameworks, Secure by Design methodologies, risk management approaches, technical assurance mechanisms, and technical solution architecture artifacts (high and low level designs).

Capgemini would typically approach enterprise security architecture by documenting:

- **The business context of the organisation and the specific programme or project –** identifying the relevant risks and requirements that provide the "why" of why security must be embedded within delivery (tied to business value where possible)
- **The conceptual security model – documenting** the "what" that the organisation needs to provide by way of security controls to meet the identified needs and counter the identified threats
- **The logical security model –** documenting the "how" the organisation can meet those needs
- **Physical security architecture artifacts –** documenting the specific technology and process controls that need to be in place.

This approach provides traceability from risk and requirement to technical implementation and enables a multitude of wider benefits such as regulatory compliance and the potential to consolidate and/or de-duplicate security capabilities, reducing the total cost of operation of the security capabilities. Capgemini can also then support the build and deployment of the documented security solutions. Capgemini is able to provide support for any stage of the programme and project lifecycle; for example, if the Buyer already has a well developed enterprise security strategy and architecture then we can simply focus on the solution architecture, design and build and align with the existing frameworks.

To support this ESP&C service, Capgemini can provide security consultants ranging from junior through to principal levels. Our consultants can also be placed in roles such as Design Authority, Technical Design Authority, Security Assurance Architect, Trusted Advisor and Procurement Support. Capgemini's security consultants can assist clients in defining the structure and organisation of a service, as well as the design, implementation and integration of associated hardware and software, including cloud delivered IaaS, SaaS and PaaS.

At the most senior levels, Capgemini's Principal Security Consultants provide thought leadership for clients and their delivery programs. They operate at senior levels within organisations, leading on the security elements of complex programmes of work, and driving close partnership between Capgemini and the client. Principal Security Consultants help client organisations understand and navigate the complexities and opportunities inherent in a complex business environment. They also help establish security architecture/assurance/delivery programmes of work, organisational governance, and technology and process designs in accordance with the principles of enterprise architecture. We can also assist clients in managing implementation of security capabilities, passing through assurance gates, and in the selection and procurement of suitable tools and services.

Capgemini's Managing and Senior Security Consultants are proficient in applying security architecture methods, threat modelling and risk assessment techniques, assurance frameworks, and design criteria and can advise others in this regard. With knowledge of one or more business domains, technical security solutions and security tools, combined with industry innovations, they can contribute to new developments in the security arena. Architects at this level are normally TOGAF 9 or TOGAF 10 certified and can operate at CIO/CTO level in client organisations. Many consultants also possess vendor certifications such as AWS Certified Solutions Architect and Microsoft Cybersecurity Architect.

Capgemini's Junior Security consultants typically operate as part of a team supporting a Security Delivery Lead. They could be cost-effective for routine security tasks rather than tying up expensive senior people on such matters.

Capgemini develops security architecture based on open/standard frameworks, such as:

- The Open Group Architecture Framework (TOGAF). This is the leading open architecture framework, though it needs to be extended to handle risks and security well;
- Sherwood Applied Business Security Architecture (SABSA). This framework is dedicated to security and provides many patterns for analysing risks and relating them to countermeasures;
- Capgemini's Cloud Services Architecture framework;
- Industry security frameworks such as ISO27001 and the NIST Cyber Security Framework.
- NCSC guidance and architecture principles.

Different clients will have different security needs and may therefore need to use different frameworks. Capgemini can work with clients to help define and agree an appropriate security framework.

This service also fully supports Cloud based projects and services.

2 Business Need

Whether as a result of new statutory or regulatory requirements, in response to new threats, to meet emerging business needs, or to deliver new Digital Cloud services, Capgemini's security consultants can work with clients to help them address issues related to risk, resilience, and security.

Adopting cloud and digital services can provide clients with new business opportunities and the ability to reach more customers. However, delivering these services may involve more third parties and channels, more security complexity and interfaces, and thus more security risks to manage. Secure integration of digital and cloud services with existing enterprise services is essential. We are also seeing increasing automation through the use of Agentic AI and GenAI, both of which introduce some novel security considerations. Often, clients need additional security advice to address this need for integration and automation and to enable, manage, operate and assure their cloud and other digital services.

The following are typical use cases where Capgemini's consultancy services can add value:

1. Delivering transformation securely, whether driven by changes to departmental responsibilities or the need to meet central mandates relating to use of AI or sovereign services.
2. Needing to share sensitive information with a diverse set of business partners. Solutions must take into account the nature of the information, relevant threats, potential impacts of compromise, the security capabilities of relevant partners (and supply chain) and the policies that need to be enforced.
3. Needing to embed security into project deliveries so that security controls are aligned with the business need and commensurate with the level of risk.
4. Providing key stakeholders with assurance that security has been appropriately considered and embedded within programme and project delivery.
5. Designing and implementing security tooling in line with relevant NCSC guidance.
6. Needing to understand the security impacts of transferring applications and data to the cloud.

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 consulting, technology, outsourcing and professional services, giving them a well-rounded and customer-centric view of security. Capgemini is a corporate member and supporter of industry bodies such as the Chartered Institute of Information Security (CIISec) and the UK Cyber Security Council and delivers a range of security services to organisations in the public and private sector. Capgemini was a significant contributor to the CSA cloud security guidance and continues to contribute to its body of work.

Capgemini use architecture development methods (e.g. TOGAF or Capgemini's Integrated Architecture Framework (IAF)) and align with international open security frameworks (e.g. ISO27001, COBIT Security Baseline, PCI DSS, ISACA ISM3, CSA and BMIS) during design. In this way Capgemini can undertake repeatable architecture engagements and produce deliverables that can be understandable to other stakeholders within the client environment. Similarly, we can employ a mix of ISO27001 Lead Implementers and Auditors where the focus of an engagement is on assurance, or a variety of vendor-certified staff where the focus is on implementation.

Capgemini has a standard approach to enterprise security architecture and similar activities, depending on the client's requirements, may apply one or more of these key steps:

- Identify the key stakeholders in the client's enterprise and agree a common vision with the client;
- Work with the client to adopt an Enterprise Security Architecture (ESA) framework and tailor it to help enable the client to deliver the vision;
- Perform risk assessments in line with preferred methodologies and Secure by Design approaches
- Work with the client to assess third party and cloud services;
- Establish and agree security architecture governance model (e.g. centralized or distributed);
- Identify and, if required, provide the skills and resources to establish the architecture capability;
- Work with the client to develop an architecture linked to the client's objectives;
- Develop a set of security services to form the overall ESA reference model (making use of existing Capgemini reference models where appropriate to accelerate delivery);
- Perform a gap analysis of current security capabilities against the ESA, and identify steps needed to close the identified and agreed gaps;
- Design and implement technology and process solution to close identified gaps or better align with expected good practice;

- Monitor key indicators of effectiveness agreed by the business.

Depending on the services purchased, Capgemini's approach can help clients achieve:

- Improved sponsorship and governance of the client's programme: involvement of senior stakeholders enabling speedier resolution of issues and greater alignment throughout the delivery organisation;
- Higher project success rate: clear statement of requirements can lead to reduced design and implementation work;
- Reduced risk of non-compliance: compliance requirements flow through into solution delivery; compliance reporting is improved through architecture traceability;
- Security that is embedded at the earliest stage of development, adopting Secure by Design principles, helping avoid the need for costly re-design;
- Reduced operational expenditure by consolidation of services: re-use lowers management costs, and metrics can help make this cost-effectiveness demonstrable;
- Tooling and processes deployed in line with NCSC guidance and vendor good practice;
- Increased agility: the business can react faster to threats, and can adopt new IT delivery models with confidence, thanks to understanding of risk and greater insight into the security impacts of change.

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 the 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**: Capgemini's consultants work from our offshore locations. This provides a very cost-effective solution with access to a large pool of related skills.
- **Onshore resources:** Capgemini's consultants work from our UK offices. This provides a cost-effective solution for buyers that require UK delivery.
- **Dedicated resources:** Our consultants work on Buyer's 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 (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 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 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 Data Privacy Solutions Engineer (CDPSE)

- Certified Information Systems Auditor (CISA);
- Certified Ethical Hacker (CEH);
- TOGAF10, 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, 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