Cybersecurity – Secure Cloud Transformation

G-Cloud 14

November 2024

Table of Contents

1 Service Overview

Capgemini Secure Cloud Transformation service comprises assessment, design, build and deployment of security solutions to help migrate, re-architect or replace existing applications within public, hybrid or private cloud environments in-line with the UK NCSC Cloud Security Principles.

This service supports programmes and projects in the identification of the security issues faced during the cloud transformation process and assists in the journey of migrating to the cloud.

Capgemini can provide skilled and experienced resources to perform the service, having been helping clients to support cloud implementations since 2009.

Typically, the assessment project duration is between two to four weeks using one or two resources.

The Cloud Security Transformation service can be applied during different phases of the service deployment and often consists of:

Identifying the current security posture of the Buyer and understanding their vision and requirements for cloud adoption.

- Risk assessment to identify the security gaps within the Buyer's estate and to determine the prioritised efforts needed for the design and deployment phase. A risk-oriented approach to information security requirements is adopted through a targeted assessment of the client's current security posture, accelerated through re-use of our security reference model. The initial scope is agreed with the client and could range from an enterprise-wide assessment through to consideration of a specific application, service or cloud solution. The aim is to quickly provide the client with a view of the maturity of their security posture and identify issues that need to be addressed at various points in their cloud transformation journey.
- For the design phase of Cloud Transformation, this service can offer a security design and review capability which results in a Technical Security Architecture Design and Build of Cloud Security Controls that will be used and implemented by build teams to deploy and then run with managed services.

For more advanced and/or mature clients, we can assist with increasing the automation capabilities within their cloud-based environments and the incorporation of security responsibilities into their continuous integration/continuous deployment (CI/CD) pipelines, often referred to as DevSecOps – putting the security into DevOps.

- This service does not solely consider technical issues, Capgemini can also provide advice and guidance on security governance structures and security management approaches. Traditional centralised security approaches are often inappropriate for multi-modal IT, Capgemini can suggest security models more suited for those adopting Dev(sec)Ops approaches.
- This service can be provided onshore or offshore.

2 Business Need

Organisations are increasingly looking towards cloud services for the provision of their IT needs thanks to the improved agility, security and flexibility offered in comparison to more traditional hosting approaches. The relative strengths of cloud hosting have been recognised by the public sector and Cloud First is now the strategic direction. This change in business operation for many organisations has resulted in businesses being required to implement Cloud Transformation programmes. Security is a key element that should be considered at the early stages to allow the appropriate foundations to be established and to prevent Shadow IT from becoming entrenched within the organisation.

Investing the time and effort into understanding the security requirements at the start of a Cloud Transformation programme assists in maximising the cost-benefit to the organisation, preventing unnecessary and potentially costly expenditure compared to security being considered in the latter stages. A failure to plan from the start can result in an organisation duplicating many capabilities prior to establishment of the formal security architecture, alongside proliferation of data on a variety of cloud services.

Capgemini can provide the following benefits through this service offer to support migrating to the cloud securely:

- Short time framework to provide targeted output that can be used to drive further investment and growth for the design and deployment (RUN) phases;
- Improved visibility and definition of shared responsibility models relating to cloud services;
- Derive and Support a Cloud Security Strategy Roadmap;
- Provide traceability between Enterprise Security and Cloud Security project requirements;
- Identifications of gaps to drive security innovation and populate strategic Roadmaps;
- Derive more value from security investments through re-use of strategic foundational components such as common identity stores or secure code repositories;
- Transformation of security governance and management structures to enable DevSecOps approaches;
- Alignment to UK NCSC Cloud Security Principles and relevant information security standards;
- Enhanced evolution of services through efficient deployment of new features;
- Highlights the mechanisms and solutions for enterprise public, hybrid and private cloud security architecture.

3 Our Approach

Capgemini can conduct a thorough gap assessment of the Cloud Security requirements by adopting a risk based approach and our cloud security reference model. The **primary considerations and advantages** for the Cloud Security Transformation services are:

- Functional and Non-Functional Requirements: Gather requirements and group them where they are similar - groups of requirements often point towards an initial set of Conceptual security services;
- Risk Assessments: Identify assets, threats and the business impacts of compromise. The need for further Conceptual security services may become apparent where not previously identified through the requirements gathering exercise;
- Architecture Frameworks: Look at architecture frameworks like TOGAF, IAF and SABSA, complemented through consideration of cloud-specific models such as those produced by the Cloud Security Alliance and NIST (alongside our own reference model). This provides a basis for wider comparison with good practice;
- Enables identification of interactions between cloud consumer, on-premises providers and Cloud providers: Elaboration of the services identified as being subject to Joint Consumer/Provider or Provider delivery responsibility leads to a better understanding of the interfaces (management, contractual and security) required between consumer, legacy provider and cloud provider;
- Physical Realisation: Once you have identified the logical requirements of a service to be hosted in the cloud then you can identify the technologies or processes that are the most appropriate fit to your needs;
- Traceable and defensible: For compliance and governance needs, traceability from either requirements or risks through to technical implementation is incredibly valuable from both an audit (internal or external) perspective and from the point of view of change management.

The **Conceptual** architectural security services are derived from the following client inputs:

- High Level Business Requirements;
- Business needs;

- Regulations and Legislation;
- High Level Risk Assessments.

Once the conceptual security services are identified, the **Logical** security architecture services are derived, based on the selection of controls from applicable standards, compliance, legal regulations and sources of good practice such as:

- NCSC Cloud Security Collection, e.g. Implementing the Cloud Security Principles
- CSA Controls Matrix - Controls from the Cloud Security Alliance (CSA) matrix;
- ISO 27001 - Provides the requirements for Information Security Management Systems (ISMS);
- ISO 27017 – Code of practice for information security controls based on ISO/IEC 27002 for cloud services. ISO 27017 provides cloud-specific guidance for 37 of the controls described within ISO 27002 and introduces seven cloud-specific controls;
- ISO 27018 – A standard for cloud service providers who process personal data. Includes around 70 controls from different international data protection laws;
- Our Cloud Security Reference Model;
- Cyber Security Essentials - The Cyber Essentials scheme, developed by UK Government and industry, provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats, within the context of the UK Government's 10 Steps to Cyber Security;
- PCI-DSS - Standard for protecting credit card data.

The next step is the selection of the **Physical** components which manifest the logical security controls. This is where in-depth knowledge of existing services and offerings and their underlying security controls is important.

The Secure Cloud Transformation can result in one (or a combination) of the following types of deliverables (based on the agreed scope):

- Identification of the tactical projects to determine the required actions to align to the cloud security roadmap;
- Integrated Risk Register to manage cloud services;
- Assurance Report following an assessment of the UK hosted Cloud Provider;
- Technical Security Architecture Design and Build of Cloud Security Controls;
- Compliance assessment report against Cloud Security standards.

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, managed by Capgemini. Please contact Capgemini to discuss which of these options fits Buyer requirements. These are:

- **Offshore resources**: Capgemini consultants work from offshore locations. This provides a very cost-effective solution with access to a large pool of related skills.
- **Onshore resources:** Capgemini consultants work from UK offices. This provides a cost-effective solution for buyers that require UK delivery.
- **Dedicated resources:** Capgemini consultants work on Buyer's sites, embedded as part of Buyer's 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 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. Typical projects (during the assessment and design phases) generally are on Fixed Price basis with typical project duration around 4-8 weeks.

Pricing agreements are subject to a scoping exercise where the Buyer is expected to complete a pre-qualification questionnaire. Capgemini will assess the complexity of the Cloud Security Transformation engagement and clarify the scope of the activity before confirming the duration and cost of the engagement.

All charges are exclusive of taxes.

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.

G13AUG22