Cybersecurity – Cloud Security Assessment

G-Cloud 14

November 2024

Table of Contents

1 Service Overview

Capgemini's maturity assessment determines the Buyer's cloud and security capability against industry best practice (e.g., NIST). Our Security transformation advisory enables the delivery of effective data-driven transformation programme. CISO Advisory Services assist the establishing of a CISO function. The Security Operating Model operationalises security strategies ensuring a robust security posture.

Features

- Defined approach, assessing cyber maturity using tried and tested methodology
- Maturity assessment of existing cybersecurity capabilities
- Alignment to industry security framework models e.g., NIST CSF
- Insights report including areas of risk and recommendations for improvement
- Holistic organisational view of cybersecurity maturity by security domains
- Prioritised recommendations including the identification of new and uplifted capabilities
- Security strategy definition: defined roadmap and business case for change
- Integration with ongoing assurance and audit requirements
- Ability to operationalise a cybersecurity maturity assessment framework

2 Business Need

Few organizations have a complete grasp of their cloud security posture. The fragmentation and erosion of a fixed perimeter caused by deployment of multiple cloud solutions in hybrid environments, alongside ecosystem complexity can lead to unclear attack surfaces for perpetrators to exploit, increasing the risk of a security incident.

The business need for the Cloud Security Maturity Assessment Service is to assist Capgemini's clients in identifying areas for improvement in their approach towards securing services hosted using cloud services. The scope of the assessment ranges from high-level governance issues such as ownership of cloud initiatives and cloud security strategy through to low-level opportunities for improvement relating to the configuration of implemented cloud services.

3 Our Approach

A Cloud Security Assessment provides you with comprehensive and holistic insight into your current cloud security posture, structured around our standards aligned reference model.

- We perform your cloud security maturity assessment through interviews, workshops, and documentation review.
- We evaluate your existing cloud based solutions (AWS, Azure, or Google Cloud Platform) against the relevant Center for Internet Security (CIS) benchmark(s).
- Maturity assessments are modular and tailorable, covering the broad spectrum of cloud security, from compliance and governance through to DevSecOps and container security.

The Cloud Security Maturity Assessment Service is modular by design, allowing clients to decide which elements of the assessment to include within scope.

The service is provided in the form of two separate streams of activity:

- **Desk-based assessment** of cloud security maturity, based on reviews of existing client documentation, discovery workshops and client responses to our cloud security questionnaire.
- **Automated policy compliance** review using the Trend Conformity tooling (or, alternatively, the posture management tooling offered by the cloud providers, i.e. AWS Security Hub, Azure Defender for Cloud, Google Security Command Center). Trend Conformity is used to assess the in-scope cloud platforms against relevant CIS benchmarks. The consultant will need to work with the client to deploy and configure the relevant access roles, operate the Conformity tooling and then assist the engagement lead by providing interpreted results from the tooling for incorporation into the final service deliverable.

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 Buyer responsibilities as part of this service are as follows:

- The Buyer will define the scope of the area to be assessed.
- The Buyer will provide any training and awareness education to the security assessor as is required by the on boarding requirements.
- The Buyer will provide a project manager to act as a single point of contact and an escalation route for the full duration of the project.
- The Buyer will make available appropriate subject matter experts and documentation (business and technical) to the project as appropriate to support the security assurance assessments.
- The Buyer will be responsible for providing detailed requirements by the mutually agreed date.
- The Buyer will announce the assessment to all appropriate individuals, asset and process owners.
- All internal and external user communications will be managed by the Buyer.
- The Buyer will accept the security assurance assessments report via post assessment presentation and be responsible for managing the recommendation identified from the assessments activity.
- The Buyer will provide the access required to in-scope cloud services to allow the usage of appropriate security assessment tooling, as directed by the Supplier.

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 (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 Partnerships/Alliances

This is an optional section where industry / strategic alliances/partnerships ***specific to this offer*** *may be mentioned. If there are none please remove this purple guidance note and the section.*

10 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 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 (CRIS)
- Computer Hacking Forensics Investigator (CHFI)
- Capgemini delivery staff hold a wide range of vendor specific certifications for many types of cybersecurity tooling.

11 Sub-contractors

Capgemini UK may use the following subcontractors to deliver this service:

- Capgemini Technology Services India Limited.

12 Business Continuity and Disaster Recovery

No disaster recovery plan is provided as part of these Services.

13 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.

14 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.

15 Termination Terms

Please refer to the Supplier Terms for this service.

16 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