Capgemini

Cybersecurity Maturity: Assessment, Strategy and Transformation

G-Cloud 15

Table of Contents

1 Service Overview

The Cybersecurity Maturity: Assessment, Strategy and Transformation service enables the Buyer to assess the current strength of their overall cloud and security capabilities. The service identifies ways to make risk-based and data-driven decisions to transform cloud and security capabilities based on the emerging trends impacting the Buyer's organisation.

This service provides Buyers with strategy and transformation advisory support as well as delivery in order to build the strategic foundations for change. There are 4 overarching offerings which exist under this service:

1. **Security maturity assessment:** perform an assessment to define the Buyer's current cybersecurity posture and determine the maturity of cybersecurity capabilities against industry best practice frameworks and standards (e.g., NIST, ISO27001, CIS, ISF benchmark)
2. **Security transformation advisory:** establish a clear roadmap for change and determine how to effectively implement security transformation to enhance the Buyer's cybersecurity capability.
3. **CISO advisory Services:** establish a CISO function or enhancing existing practices
4. **Security Operating Model (SOM):** operationalise security strategies and frameworks across teams, processes, technology and data to help deliver a robust security posture and alignment with industry best practices.

With these offerings, our goal is to empower your organisations and elevate your cybersecurity posture, ensuring strategic alignment with industry standards and best practices for a secure and resilient future.

2 Business Need

Alongside the growing threat landscape, many organisations face a number of challenges when delivering security strategically:

- Organisations may have a multitude of **disparate security, risk and compliance assessments** resulting in duplication, inefficiencies and siloed security operating models.
- **The external threat landscape** is continuously changing and organisations' modes of delivery struggle to keep pace with new threats. A traditional "set it/forget it" cybersecurity approach is no longer effective in today's challenging threat environment.
- **Poor visibility** of the effectiveness of security practices; **not getting value for money** in the technologies that organisations are employing.
- Unmanaged risks across the organisation (**blind spots** across the business) e.g. supply chain and third-party risks
- Lack of direction and **alignment to business objectives**
- Difficulty navigating new and **complex regulation**

Security programs driven by technology and regulatory compliance alone are no longer adequately protecting organisations that possess and transmit high-value intellectual property and personal information.

Understanding the Buyer's organisation business goals is critical to identify where to prioritise investment in improving security capabilities.

3 Our Approach

Capgemini would help identify and develop the Buyer's security strategy and work together with the Buyer to establish the preferred approach for business change; this will allow Capgemini to tailor the service to Buyer's requirements. Our offerings under this service can help the Buyer at any stage of their security transformation

journey: from initial maturity assessment through to transformation roadmap creation and reviewing existing security operations.

3.1 Security Maturity Assessment

Capgemini's security maturity assessment capability analyses the Buyer's current cybersecurity capability against the industry best practice (NIST, ISO27001, CIS, ISF benchmark) and the Buyer's own cybersecurity policies and frameworks. This evaluation is appropriate for Buyers with foundational framework processes in place for NIST, CIS 18 and/or ISO 27001 or Buyers who wish to align current assessment activities to these specific standards for the first time. Buyers can leverage this evaluation to assess themselves against security best practice, determine their current and target security profile, compare their cybersecurity maturity posture to that of their sector peers and justify future security programme activity.

Key Outcomes:

- Establish control of ownership and roles and responsibilities (Departments, Directorates, Business Units/Areas, Capability Teams).
- Assessment to determine existing levels of control coverage and identification of areas where further information and insight is required.
- Understanding security maturity against industry peers to set benchmarks including gap analysis to highlight areas of strength and help identify areas of weakness.
- Translated recommendations born out of the assessment into a series of change activities and identified macro delivery initiatives.
- Conceptualised 'programmes of work' for each initiative to help address a particular deficiency identified in the assessment.

3.2 Strategic Transformation Advisory

Capgemini's strategic transformation capability utilises data and insights from security maturity assessments, market research and user engagement to support the definition of a target state for the Buyer's organisation's cybersecurity function.

Based on the insight derived from this analysis, Capgemini can help define and implement relevant programmes and remediation plans to meet the Buyer's strategic objectives. Capgemini's approach supports Buyers in determining their security strategy through the assessment of different parameters (i.e., maturity shortfalls, strategic priorities, strategic risks), identification and design of necessary transformation activities and delivery of a high-level strategic roadmap.

The security transformation roadmap can be delivered via a portfolio of programmes and projects, reported on and measured over time to track measurable improvements in security maturity based on strategic programme outcomes.

Key Outcomes

Discovery of insights report which provides an overview of Buyer's drivers for change and views on target security strategy.

- Identification of change management activities to realise target security strategy and vision (people, processes, data, and technology). Advisory services to implement and deliver change management services
- Assist in generation of business cases to build an agreement for change among key stakeholders.
- Established security MI and data insights to monitor maturity progress through lifecycle of transformation plan
- Help the Buyer's organisation identify key milestones and associated risks to be monitored throughout the delivery of the roadmap

- Develop the Buyer's security strategy (incl. rationale, analysis, business case and future milestones as driven by the provided recommendations)

3.3 CISO Advisory Services

Capgemini's CISO Advisory Services provide a comprehensive spectrum of services to build and increase the impact of the CISO function, to keep them more secure and protect their reputation. With business requirements and cybersecurity threats constantly changing, organisations and CISOs need to realign their priorities to uphold a security culture that enables business growth. Capgemini's experienced specialists will engage with the Buyer's CISO and security resources in a wide range of activities, from establishing a diverse and blended best-in-class security team developing the appropriate skillsets, to preparing the CISO in transition from the meeting rooms to the board rooms. Capgemini's security journey is based on a collaborative business experience to create and establish a security culture integrated within the business strategy and future transformation.

Key Outcomes:

- Delineated and empowered CISO role and function with clear responsibilities and recognised authority within the organisation through effective governance realignment, enabled by a clear cybersecurity strategy
- Definition and implementation of the CISO function's operating model, based on the buyer requirements, as-is situation, and strategic objectives
- In-depth assessment against predetermined benchmarks (e.g., ISO27001, NIST) that defines desired future state and priorities for the CISO
- Design and optimise security processes which drive operational resilience and business efficiency

3.4 Security Operating Model (SOM)

Capgemini's SOM offering is designed to operationalise cybersecurity strategies and frameworks across teams, processes, technology and data to help deliver a robust security posture and alignment with industry best practices. This embeds security measures across all levels of the organisation, fostering resilience, and proactive threat mitigation. Central to the SOM is a defined governance process which enables teams, the processes they carry out and the technologies they utilise to work in unison as data-driven way. In this way, silos amongst the security function are avoided and security activities are carried out efficiently. An effective SOM helps organisations to manage security risks and enhance their cybersecurity posture through continuous assessment and improvement initiatives. Capgemini can comprehensively assess the existing SOM and define the target SOM whilst identifying areas of improvement for security operations across the Buyer's organisation

Capgemini can support the buyer to implement innovative technologies to enhance SOM efficiency. For example, automating reporting to help with security governance while tracking KPIs and extracting insights from SOM data. The SOM enables an optimised transformation portfolio with robust governance controls, tracking the impact of security programs on maturity. Feedback from transformation efforts is looped back into assessment and risk frameworks, facilitating ongoing risk reduction over time.

Key Outcomes:

- Assessment of existing SOM and definition of target SOM: teams, processes, technology and data to identify gaps and recommendations for operational improvements
- Comprehensive view of security compliance requirements, aligned to organisational policies and standards, across buyer's organisation.
- Refined stakeholder engagement to drive ownership and management of security assessment activities.
- Upskilling security teams and stakeholders to operate assessment tools proficiently.
- Establishment of risk-aligned metrics and domain prioritisation to address security gaps.
- Increased visibility of current and target maturity levels across security domains.
- Holistic view of operational security for senior leadership through centralised reporting dashboards.

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 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) and business owners 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:

- **Onshore resources:** Capgemini consultants work from our UK offices. This provides a cost-effective solution for buyers that require UK delivery.
- **Dedicated resources:** Capgemini 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 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.

ISO 9001 Quality Management for Management Consultancy and IT Implementation and services to the Public Sector

ISO 27001:2013 - Provision (Delivery) of IT services including business applications development, maintenance and Data, Digital and Cloud technologies.

NelsonHall has identified Capgemini as a Leader in its 2022 NEAT Vendor Evaluation for Learning Services due to its ability to meet future client requirements as well as its capability to deliver immediate learning benefits to them.

Capgemini is the first amongst consultancy and technology firms to be recognized six times in a row for its thought leadership reports.

2023 Ecovadis Platinum Rating: We maintained a platinum rating, recognising us as a responsible and sustainable business in the top 1% of companies assessed.

Better Society Awards: Our collaboration with Code Your Future to offer digital skills training won a Better Society Award in 2022. The awards celebrate efforts by commercial organisations to create a better society.

Inclusive Top 50 UK Employers List: We achieved second place in the Inclusive Top 50 UK Employers List 2022/23 – a list that assesses companies for best practice on diversity, equality and inclusion

UK Best Workplaces for Women: We were listed as a Best Workplace for Women by Great Place to Work®. This listing is based on responses from our team to an anonymous survey about their employee experience.

UK Best Workplaces for Wellbeing: We are listed by Great Place to Work® as a Best Workplace for Wellbeing

Great Place to Work: We were certified as a Great Place to Work® in 2023, reflecting our employees' experience of working at Capgemini in the UK.

Capgemini can provide security delivery professionals with the following industry certifications:

- CESG Certified Professional (CCP).
- 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 Institute of Information Security Professionals (IISP)
- NIST Cybersecurity Framework (NCSF)
- Certified in Risk and Information Systems Control (CRIS)
- Computer Hacking Forensics Investigator (CHFI)
- Capgemini has also received NCSC certified cyber security consultancy status.

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

Capgemini can provide a range of cyber security services such as – cybersecurity awareness, behaviours and culture, security management, governance risk and compliance, architecture design & implementation, identity and access management, cyber analytics & protective monitoring, digital forensics and testing.

Capgemini has over 500 security professionals based in the UK whose expertise can be leveraged to provide our Buyer's with cyber security services.

For more information about this or any of Capgemini's 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