Cyber Risk Assessment G-Cloud 14

November 2024

Table of Contents

1 Service Overview

A Cyber Risk Assessment for the cloud involves a systematic process of identifying, evaluating, and prioritizing potential risks that could affect an organisation's objectives, assets, infrastructures, or processes. Capgemini's Cyber Risk Assessments involve analysing the likelihood and impact of various risks, considering both internal and external factors. The goal is to inform decision-making and develop strategies to mitigate or manage identified risks effectively, enabling the organisation to achieve its goals while minimising potential negative impacts. Risk assessments are crucial for proactive risk management and are commonly used in areas such as information security, project management, finance, and overall organisational planning.

2 Business Need

Cyber Risk Assessments are essential for organisations in today's digital environment as they provide a comprehensive understanding of potential vulnerabilities within systems, networks, and processes. By proactively identifying and prioritising risks, businesses can allocate resources effectively, enhance compliance with regulatory standards, and safeguard sensitive information from data breaches.

Capgemini's assessments can contribute to the development of robust incident response plans, fostering a cybersecurity culture among employees. Additionally, they enable cost-effective resource allocation, ensuring that limited resources are invested in technologies, training, and policies that address the most significant risks.

The continuous improvement cycle facilitated by regular assessments helps organizations stay ahead of evolving cyber threats. Furthermore, Cyber Risk Assessments play a crucial role in transparently communicating risk implications to key stakeholders and may influence insurance considerations. Overall, they are a cornerstone of a comprehensive cybersecurity strategy, providing a structured approach to managing and mitigating cyber risks.

The benefits of completing a cloud-based Cyber Risk Assessment can help organisations:

- Identify and understand potential vulnerabilities in their systems.
- Prioritise their cloud security measures based on the severity and likelihood of potential vulnerabilities.
- Identify industry and regional specific regulations and compliance standards related to cybersecurity.
- Understand potential risks to develop and refine incident response plans.
- Identify potential threats to enable quicker and more effective responses to cyber incidents, minimizing potential disruption.
- Demonstrating a commitment to cybersecurity through assessments may result in more favourable insurance terms.

3 Our Approach

Our approach is split into 7 key areas:

- Phase One – Project Kick Off
  - Confirmation of the overall objective and timelines
  - Identification of key personnel.
  - Confirmation of the scope.
  - Confirmation of risk posture.
  - Align to the organisations risk approach and definitions.
- Phase Two – Asset Identification & Document Review

- Identify and catalogue all critical assets, including hardware, software, data, and networks.
- Classify assets based on their importance and sensitivity to the organisation.
- Confirmation of the plan with the primary contact.
- Review all existing documentation in place in relation to risk management.

- Phase Three – Threat and Vulnerability Identification
  - Identify potential threats and vulnerabilities that could impact the organisation.
  - Analyse external and internal sources for emerging threats and vulnerabilities.
- Phase Four – Probability Analysis
  - Evaluate the likelihood of identified risks.
  - Assign risk scores based on a combination of factors, such as threat severity, vulnerability, and the effectiveness of existing controls.
- Phase Five – Risk Identification & Impact Analysis
  - Assess the likelihood of each identified risk scenario occurring.
  - Evaluate the potential impact on the organization in terms of financial, operational, and reputational consequences.
- Phase Six – Priority and Mitigation
  - Prioritise identified risks based on their severity, potential impact, and likelihood.
  - Establish a risk register that ranks risks according to their priority for mitigation.
  - Develop and implement strategies to mitigate identified risks.
  - Prioritize mitigation efforts based on the severity of risks and available resources.
- Phase Seven – Summary Report
  - Document the entire assessment process, including findings, methodologies, and recommendations.
  - Prepare a comprehensive report for key stakeholders, outlining the organisation's risk profile and proposed mitigation strategies.
  - Implement a continuous monitoring process to track changes in the threat landscape and the effectiveness of mitigation efforts.

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) as appropriate to support the project or delivery plan;

The Buyer will make available all appropriate documentation for review in a timely manner in line with the Project Plan.

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 Capgemini to discuss which of these fits Buyer's requirements. These are:

Onshore resources: Capgemini's consultants work from it's UK offices. This provides a cost-effective solution for buyers that require UK delivery.

Dedicated resources: Capgemini's consultants can 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 (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 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:

- CESG Certified Professional (CCP);
- Certified Information Privacy Professional/Europe (CIPP/E);
- Certified GDPR Practitioner;
- Certified Payment Card Industry QSA Assessors (PCI-DSS);
- 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);
- 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 NCSC certified cyber security consultancy status. Details are available on the NCSC website at this link: https://www.ncsc.gov.uk/professional-service/cyber-security-consultancy-capgemini-uk-plc.

10 Sub-contractors

Not applicable to this service.

11 Business Continuity and Disaster Recovery

No disaster recovery plan is provided as part of this service.

12 Pricing

This service is priced in accordance with the SFIA Rate Card attached. 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.

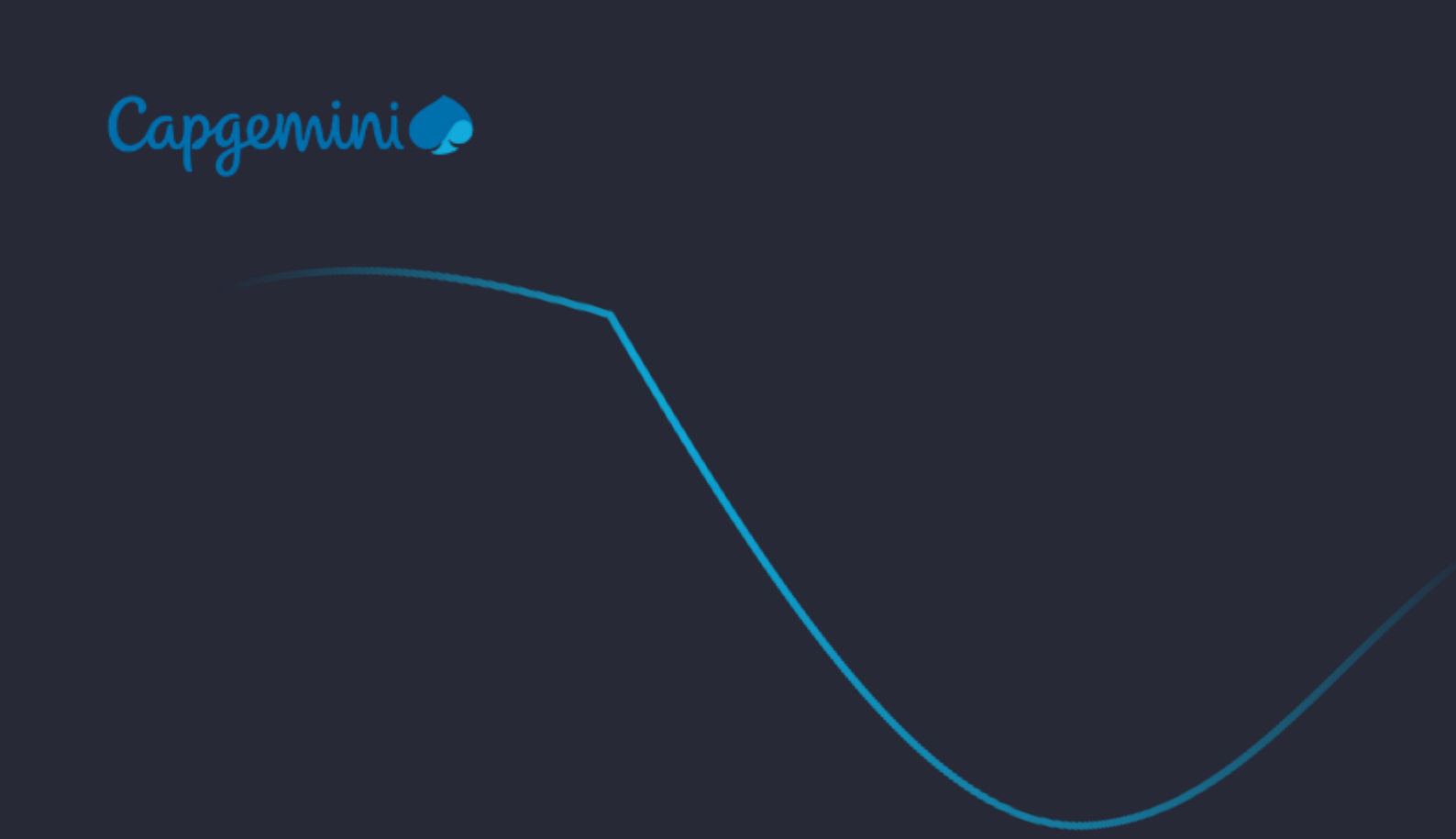
15 Further Information

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, 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