Capgemini

Third-party (Supplier) Security Assurance and Compliance

G-Cloud 15

Table of Contents

1 Service Overview

1.1 Third-party (Supplier) Security Assurance and Compliance as a Service

The Capgemini third-party security assurance service comprises a set of strategies, policies, processes and an underlying set of controls that can support the protection of its clients' information assets in enterprise and cloud environments. Capgemini can help client's to meet their supply chain security assurance requirements via the provision of sustainable and repeatable practices and measures certified by IASME as being aligned to the Cyber Essentials scheme.

Third-party security assurance is important in cloud environments where clients can have one or more third parties delivering key services, demanding security assurance oversight of the integration and linkages across such services.

Capgemini understands the challenges of cyber security in the 21st century and has a dedicated team that can support its clients' third-party compliance and security assurance needs.

The Capgemini security team is comprised of Security Check (SC) and Developed Vetting (DV) cleared ISO27001 Lead Auditors and Implementers, Certified Information Security Managers (CISMs) and Certified Information System Auditors (CISAs), able to provide a service tailored to client requirements. Conducting risk and compliance maturity assessments can help enable Capgemini and its clients to jointly prioritise activities around key vulnerabilities and high risk business functions to maintain Confidentiality, Integrity and Availability (CIA) of clients' services.

Capgemini's collaborative engagement with a cross-section of clients over many years has resulted in a team that can get to the heart of third-party security assurance needs. Capgemini can work with clients and third parties to understand and guide their risk management strategies and can help them treat identified weaknesses.

Capgemini's consultants can undertake risk-based maturity reviews of the security regimes operated by existing and prospective third-party suppliers. This can enable Capgemini to help the client gain assurance that the supply chain is secure and does not have the potential to expose the client's business to unacceptable levels of risk.

Capgemini can offer a mature range of assurance services across all aspects of third-party and cloud security. The service can be tailored to specific client's operational requirements.

Whether third parties are engaged to provide cloud services, operate high security data centers, develop tailored code for the client's networks, receive data for large-scale print output requirements or offer agency personnel to enable clients to flex their staffing and skilled resources, etc. the Capgemini security team can advise and provide support.

2 Business Need

In any business the engagement of third-party suppliers can present significant threats to data security. While each client has the capability to determine security policies and enforce them within its own workforce, ensuring that these are operated and enforced within the supply chain presents its own challenges.

The extension of a client's security culture into its supply chain can be addressed through contracts and non-disclosure agreements (the foundations of good security practice). However, once that initial engagement has been completed, there remains an on-going need to ensure that the supplier's internal security culture and practices do not risk compromising the security of the client's business.

This is an area of increasing risk, as evidenced by recent security breaches which have involved attackers targeting weak security controls and cultures within 3rd Party suppliers in order to compromise the true target.

The through-life validation and monitoring of the data security compliance of 3rd Party suppliers will also play a significant part in an organisation's ability to demonstrate its regulatory compliance with the GDPR.

Capgemini's third-party security assurance consultants can work collaboratively with its clients to provide a proportionate, practical and effective service with strategies tailored to the agreed contractual requirements in order to support the agreed technical, physical and procedural security controls in place.

The Capgemini third-party security strategies can help to promote adherence to established security policies wherever the client's information assets are handled, thereby reducing the potential within the supply chain for:

- The theft or loss of the client's physical or information assets;
- Damage to such assets in order to disrupt the client's operational capabilities or discredit the client;
- Malicious changes to the products provided, such as the corruption of data or the addition of unauthorised components to any hardware provided;
- Security complacency through failures to promote effective security training and awareness within the supplier's workforce.

Capgemini's third-party security assurance and compliance service is delivered through robust consulting methodologies, based on its expertise and experience in this field.

3 Our Approach

Capgemini security professionals have a wealth of experience in UK Government and private industry security assessments including qualified ISO27001 Lead Auditors.

Security assessments can be tailored to the contractually agreed requirements of the client, but can include any of the following:

- ISO27001 assessments ahead of a certification audit by one of the approved certification bodies;
- Review of compliance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679);
- Physical security and procedural assessments structured around the ISO27001 standard;
- National Protective Security Authority (NPSA) Operational Requirements (OR) Level 1 & 2 assessments, particularly for new third-party services and premises;
- Information Security Forum (ISF) Security Maturity Model assessments using the ISF Accelerator Tool, particularly where there are multiple vendors providing connected services to the client;
- HM Government Security Policy Framework (SPF) and Government Functional Standard GovS 007: Security Supplier Assurance Framework assessments. These can be conducted as high-level self-assessments or low-level objective assessments conducted at the suppliers' premises;
- Collaborative reviews on behalf of HM Government clients in the preparation of environments to meet List X requirements.

Dependent on the size and complexity of the client's supply chain, a risk-based combination of several of the methods detailed here can be deployed and managed under the umbrella of an agreed third-party security assurance programme.

Typically, the following lifecycle of activities can be agreed and implemented:

- Initial scoping conducted to determine and develop the right strategy for the client;
- Threat analysis;
- Joint third-party security assurance and compliance programme planning;
- Use of a range of agreed industry good practice methodologies tailored to client's needs;
- Support provided to devise and conduct risk assessments & gap analysis;

- On-site or questionnaire-based assessments of controls in place;
- Reviews of findings and production of reports with recommended actions;
- Monitoring of, and support for, treatment of recommendations raised;
- Testing of implemented controls, where agreed and appropriate;
- Periodic follow-up assessments to agreed timeframes.

The approach is designed to help deliver the following client benefits:

- A coherent, risk-based third-party security assurance and compliance strategy;
- Assurance that supplier security regimes are consistent with the client's security policies and regulatory requirements;
- Identification and resolution of security vulnerabilities;
- Provision of cost-effective solutions, where security enhancements are necessary;
- A reduction in the number or likelihood of security incidents and related mitigation costs;
- Use of industry good practice methodologies;
- A scalable solution to address simple to complex supply chain models.

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, all fully managed by Capgemini. Please contact Capgemini to discuss which of these fits Buyer's requirements. These are:

- **Offshore resources**: Capgemini consultants work from Capgemini offshore locations. This provides a very cost-effective solution with access to a large pool of related skills.
- **Onshore resources:** Capgemini consultants work from Capgemini 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 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 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 (CRISC)
- 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 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