Capgemini

PCI DSS Compliance (QSA services)
G-Cloud 15

Table of Contents

1 Service Overview 3
2 Business Need 3
3 Our Approach 3
4 Buyer Responsibilities 4
5 Service Management 5
6 Protection of Data 5
7 On-boarding and Off-boarding 5
8 Skills and Knowledge Transfer 5
9 Vendor Accreditations/Awards 5
10 Sub-contractors 6
11 Business Continuity and Disaster Recovery 6
12 Pricing 6
13 Ordering and Invoicing 6
14 Termination Terms 6
15 Further Information 6

1 Service Overview

Capgemini is a Qualified Security Assessor Company (QSAC) and have extensive experience in carrying out assessments against the PCI-DSS standard for both merchants and service providers, including cloud hosting companies, as well as reviewing self-assessment questionnaires for entities who are eligible to complete self-assessments.

The deliverables for a formal PCI-DSS assessment includes completion of the Report on Compliance (RoC) or Self-Assessment Questionnaire (SAQ) for Assisted Self-Assessment, and the Attestation of Compliance (AoC).

2 Business Need

All merchants and service providers that process, transmit or store cardholder data must comply with the PCI DSS. There are many benefits from meeting its requirements:

- Builds trust with organisations customers.
- Prevents data breaches.
- Helps organisations to meet global standards.
- Puts security first.
- Provides a baseline for other regulations & Standards.
- Avoid fines and penalties.

Compliance with PCI-DSS is usually a requirement laid out in the merchant's contract with their acquiring bank. Penalties for non-compliance can include increased fees, financial penalties and, in extreme cases, the withdrawal of the merchant's ability to take payments via payment card.

Additionally, compliance is required for third-party service providers including, but not limited to, third parties that:

- Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers [PSPs])
- Manage system components included in the entity's PCI DSS assessment (for example, via network security control services, anti-malware services, security incident and event management [SIEM], cloud hosting companies, IaaS, PaaS, SaaS, FaaS, etc. and other cloud enabled services)
- Could impact the security of the entity's account data (for example, vendors providing support via remote access, and/or bespoke software developers).

The assessment is required to be carried out on an annual basis.

3 Our Approach

Capgemini's standard assessment methodology includes the following phase and are refined to meet buyer requirements and objectives:

- Phase One – Opening Meeting
  - Confirmation of the overall objective(s) of the assessment
  - Confirmation of timelines
  - Identification of key personnel
  - Confirmation of the scope (including systems, processes, people and locations)
- Phase Two – Planning

- Creation of a plan of assessment activities and interviews
- Provision of details of topics to be covered with key personnel.
- Creation of a sample list for requirement documentation and evidence
- Dissemination of a schedule of activities with personnel
- A confirmed schedule for the report creation & QA activities
- Confirmation of the overall plan with the primary contact

- Phase Three – Assessment
  - Assessment of compliance with the control requirements in line with the PCI-DSS standard
  - Interviews, documentation reviews and observation testing as required by the standard including of that of third parties i.e. Cloud Service Provider (CSP) compliance.
  - Communication and escalation of any non-compliances identified to enable swift remediation (Where applicable)
  - Verbal summary of the days finding with the primary contact at the end of each day
- Phase Four – Report writing and a three-stage QA Process
  - Completion of the Report on Compliance (RoC), the Attestation of Compliance (AoC) and an Items Noted for Improvement (INFI) report.
  - Technical review by another QSA (QA1)
  - Report review (QA2)
  - Finalisation (QA3) and signature of the report before release to the customer
  - Remediation plan for any non-compliances identified, including timescale of remediation and re-assessment.
  - Close out meeting (If required)
- Phase Five – Remediation support (If required)
  - Where a non-compliance is identified that cannot be resolved during the assessment, a non-compliant report will be provided, detailing the compliant controls in place as well as the identified non-compliance.
  - The non-compliance is required to have a remediation date confirmed, the enable the remediation assessment of the requirement to be carried out as soon as practical to enable the delivery of a compliant report.
  - Capgemini can provide technical support as well as QSA support in investigating, identifying and implementing suitable remediation(s) for any non-compliances or anomalies.

4 Buyer Responsibilities

All buyer responsibilities are identified and detailed in any project plans and statement of work.

Standard responsibilities include:

- Providing points of contact throughout the engagement
- Adherence to all requests for information, including written (hard copy\electronic) and verbal
- Access to appropriate facilities, technologies and individuals

5 Service Management

Capgemini will allocate a dedicated PCI-SSC certified QSA for the assessment.

Dependant on the scope, location, and complexity of the assessment, the QSA may be supported by additional resources as required to complete the assessment.

This may include specialist technical and non-technical resources and may be provided from Capgemini's onshore or offshore resource pools as appropriate.

The use of any additional resource will be agreed with the primary contact prior to any commencement, and with full oversight by the dedicated project QSA.

Points of escalation will be communicated prior to commencement of any activities to ensure swift resolution of any issues.

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 the 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.

Qualified Security Assessor (QSA) companies are independent security organizations that have been qualified by the PCI Security Standards Council to validate an entity's adherence to PCI DSS. QSA employees are individuals employed by a QSA company and have satisfied and continue to satisfy all QSA requirements.

Capgemini and its Qualified Security Assessor statuses are listed on the PCI-SSC's website for validation purposes.

10 Sub-contractors

Subcontractors are not used for the provision of 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. 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