Cybersecurity - Security and Regulatory Assurance - Advice and Build

G-Cloud 11

July 2019

Table of Contents

Service Overview 1
Project Build, Development Environments 1
Business Need 1
Our Approach 2
General Features 2
Service Management 3
Protection of Data 3
On-boarding and off-boarding 3
Skills and Knowledge Transfer 3
Vendor Accreditations/Awards / Certifications 4
Sub-contractors 4
Additional Associated Services 4
Business Continuity and Disaster Recovery 4
Pricing 4
Ordering and Invoicing 5
Termination Terms 5
Further Information 5

The information contained in this document is proprietary. Copyright © 2019 Capgemini. All rights reserved.

Service Overview

Capgemini can provide skilled information assurance cyber-security professionals to help assess your information security and Regulatory compliance by providing specialist covering Cyber Security, HMG Policy, CESG guidance, ISO27001,Trade and Export, PCI DSS, Privacy/GDPR, Sarbanes Oxley assurance expertise for enterprise and cloud environments.

Our Security Assurance Managers are experienced with HMG Information Assurance Standards, CESG 'Good Practice Guides' , security and ISO 27001 assurance and compliance, both in run environments.

Security assurance assessments will provide business owners and stakeholders of their compliance position with the Security, regulatory and legislative needs of the business and provide a view of risks, liabilities, and responsibilities of your G-Cloud Service Provider with regards to your critical assets and sensitive data and systems and can be undertaken during the Project/ Build Development stages to deliver compliance into run.

Typical durations are described below but start from 1 week for a small engagement.

This offer supports Cloud based projects and services.

Project Build, Development Environments

Our security assurance managers will work with project & build teams to help ensure:

- Controls, processes and procedures are implemented in line with the Policy (e.g. HMG Security Policy Framework or local policy), security standards, ISO27001 compliance and regulatory compliance such as PCI DSS, Trade and Export, PII/GDPR requirements, during development of the project / build;
- Testing covers key aspects of security, including organising and coordinating external testing e.g. penetration testing, and sourcing and use of test data is done in an appropriate manner;
- Service introduction activities fully cover all security policy and standard requirements.

In general security assurance managers will:

- Act as a central point of contact for security assurance matters;
- Provide considered security advice, threat assessment and security assurance advice as required;
- Support accreditation (e.g. ISO27001 certification) and similar activities;
- Act as a trusted extension of the organisation's security and compliance teams;
- Report assurance and compliance status to stakeholders.

Business Need

Security is increasingly complex and subtle and new regulations (e.g. GDPR) and changes to existing legislation mean that the security and regulatory environment needs constant assessment to ensure adherence and compliance. The threats against organisations and their information have never been higher.

Information Assurance (IA) Assessments provide business owners with the confirmation of their compliance and risk position, verifying that controls are operating effectively to protect the confidentiality, integrity and availability of information systems in line with the applicable policy and standards and in line with HMG Policy and CESG Guidelines as well as international standards and applicable legislation.

The information contained in this document is proprietary. Copyright © 2019 Capgemini. All rights reserved.

The IA activity can

- Check Compliance and adequacy of protection of the systems and data throughout the lifecycle;
- Assess adequacy of Processes and procedures in line with policy / International standard requirements;
- Identify Security weaknesses in the organisations security management systems and working practices;
- Identify inadequate security in Infrastructure, applications and systems;
- Check controls applied in development and change management;
- Check adequacy of reporting and governance.

The increase in the identification of security incidents and events has also led to a massive demand for security professionals world-wide. This means that recruiting security assurance managers can be problematic especially at short notice or for part-time engagements. Capgemini's security teams are mutualised and in place which gives the flexibility that direct recruitment cannot provide.

Our Approach

Capgemini provide our security assurance managers from mutualised teams. We can provide the service as a project or as a part-time or full-time activity, and either normal business hours or 24x7.

Using mutualised teams means that service can be maintained in the event of sickness or holidays, and it also makes available a wider pool of security knowledge and experience. We also have assurance managers with specific certifications or experience.

While for many HMG organisations on-shore resourcing will be appropriate, we can also provide near-shore and off-shore resources for this service.

We cover the following areas:

- HMG Policy and Standards;
- International standards (e.g. ISO27001);
- Risk Assessment, Risk Management and Risk Treatment Options;
- Information Security and Regulatory Assurance /Compliance assessments;
- Regular Review Cycles;
- Security Management Plan development and Remediation Planning, in line with the risks/non compliances identified as a result of the security assessment.

Depending on the size of the scope an assessment can take varying periods to complete e.g.

- Small engagement – 1 week up to 1 month assessment;
- Medium engagement – up to 2 month assessment;
- Large engagement – Over 3 month's assessment.

General Features

- Can support ISO 27001, SPF compliance & accreditation activities (RMADS, IAS1/IAS2);
- Security Assurance Managers can call on wider Capgemini security community for support;
- Can support other stakeholders e.g. Information Governance, DR/BC, Caldicott Guardians;
- Can quickly adapt to meet changing Policy, Legislation and Regulations and business requirements;

The information contained in this document is proprietary. Copyright © 2019 Capgemini. All rights reserved.

- Provides a clear well-defined point of contact for security assurance matters;
- Can support implementation of Information Assurance Standards, Good Practice Guides;
- Can provide assurance managers qualified ISO27001:2013, CISSP, CISM, CISA, TOGAF9, ITIL, SABSA;
- Can provide assurance assessments covering G-cloud security / use, third parties and IEP;
- Can provide assurance assessments of Regulatory requirements e.g. address DPA/ GDPR compliance requirements.

Service Management

Capgemini Service Management provides a set of specialised organisational capabilities for providing value to clients in the form of services. It includes a full lifecycle approach to service management from service take-on, through strategy to operation and continual improvement. It can be offered either as a standalone service or in conjunction with other sourcing arrangements

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.

On-boarding and off-boarding

Prior to the execution of the Order, the Supplier and the Buyer will agree the scope of the exit plan for the Services and a timescale for delivering an exit plan to ensure continuity of service.

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.

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.

The information contained in this document is proprietary. Copyright © 2019 Capgemini. All rights reserved.

Vendor Accreditations/Awards / Certifications

Capgemini has been independently audited and certified to be in conformance with the below mentioned industry standards:

List X, ISO 27001: 2013, ISO 9001: 2008, ISO 20000-1:2005, ISO 9001: 2000, AS9100, TL9000

Sub-contractors

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

- Capgemini Technology Services India Limited.

Additional Associated Services

The following list shows a variety of additional associated services offered through G-Cloud. Additional Associated Services shall be priced based on the price defined in the offer.

- Security and Regulatory Assurance – Run Services
- Security Management - Advise and Build
- Security Management - Run Services
- Security Operations Centre (SOC) Design, Build and Accredit
- Cyber Security – Transition and Transformation
- Cyber Security Operations Centre (CSOC) – Diagnostic Assessment
- Network Asset Visibility and Illumination – Assessment
- Web Application Firewall (WAF) - Design and Implementation
- Secure Cloud Transformation
- Cyber Attack Simulation

Business Continuity and Disaster Recovery

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

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.

All charges are exclusive of taxes.

The information contained in this document is proprietary. Copyright © 2019 Capgemini. All rights reserved.

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.

Termination Terms

Please refer to the Supplier Terms for this service.

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.

The information contained in this document is proprietary. Copyright © 2019 Capgemini. All rights reserved.

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.

Visit us at www.capgemini.com.

People matter, results count.

People matter, results count.

This message contains information that may be privileged or confidential and is the property of the Capgemini Group.

Copyright © 2019 Capgemini. All rights reserved.

Rightshore® is a trademark belonging to Capgemini