Cloud Security Configuration Review

SERVICE DEFINITION FOR THE G-CLOUD 15 FRAMEWORK

Overview

Cyberis offers an extensive range of technical security assessments to the public and private sector. Our cloud security configuration reviews are designed to identify areas of cloud implementations that divert from industry and vendor guidance on best practice standards providing practical improvement guidance in the context of your business.

Personnel

Our consultancy team is highly qualified and very experienced, holding certifications including Cyber Scheme Team Leader (Infrastructure), CREST Certified Application Tester, Cyber Scheme Team Leader (Applications) and CREST Red Team Specialist. Our team also includes individuals with Chartered Cyber Security Professional (ChCSP) status, as well as a number with Principal level and below. These security testing qualifications are supported by a wide range of cloud vendor-specific technical qualifications.

Reviews are undertaken by experienced CHECK/CREST/Cyber Scheme accredited staff, with HMG SC Clearance.

We have considerable experience working on cloud security implementation review engagements across a wide variety of industry sectors.

Cloud Security Configuration Review Engagement Model

All configuration reviews are tailored to the unique requirements of the system risk, the project, the organisation and/or the Accreditor, and other related stakeholders. We will have an initial scoping call or meeting with you and your stakeholders to discuss the systems and applications under assessment, the business threat landscape, principal security concerns, and the technical assurance requirements. From this, we will produce a formal Statement of Work within a commercial proposal which will be subject to customer review and acceptance. Engagements are priced on a day rate basis – see the Pricing document for more information.

We approach every assessment differently, depending on your setup and needs. Common approaches we adopt include:

- Cloud configuration review – we provide configuration auditing, technical assessment and advice that supports moves towards hosting functions, services and data at all major cloud platforms – including AWS, Azure and Google Cloud Platform.
- Integration assessments – we identify if components are functioning according to the security assumptions made, if gaps in controls have been put in place, and any unconsidered risk

Cyberis Limited
Unit E, The Courtyard, Tewkesbury Business Park, Tewkesbury, Gloucestershire, GL20 8GD
T: +44 1684 353514 | E: info@cyberis.com | W: cyberis.com

exposures caused by existing integrations. We can help make sure you get it right, integrating services and solutions from different cloud providers, or between cloud providers and on-premise systems, presents an information security challenge.

- Remote working models – with more staff working from home, you may be using cloud platforms to provide email, file sharing and communications platforms. We can assess how exposed sensitive data might be to external adversaries if credentials are compromised, or if devices are infected with malware.
- Common cloud platforms – we regularly conduct security configuration and implementation reviews of common cloud platforms including Entra ID, Microsoft Intune and Microsoft 365 to identify where security configurations divert from industry and vendor recommended good practice, or where security could be enhanced.
- Cloud Risk Management consultancy – support and guidance with applying vendor and industry good practice to your specific implementation, risk appetite and business needs.
- Cloud Breach Assessment – identification of indicators of compromise following a suspected breach, with support to understand the extent of a breach, remediate and improve security moving forward

We address each of these risks through focussed, hybrid approaches – including IaaS, PaaS and SaaS technologies. This involves combining the assessment of controls at each level to understand overall risk, and using threat-driven scenario-based assessment to capture and fix end-to-end security risks.

As part of a Cloud Security Configuration Review, we can also include other technical assurance elements, including penetration testing (including IT Health Checks where appropriate) and virtual host build/configuration assessments and reviews.

Assessments and reviews may be based on government standards and guidance, industry standards, internal standards, principal security concerns and/or specific system requirements as required to meet stakeholder technical assurance objectives.

The results of a cloud security configuration review can be fed into your organisation's risk management process, and can help to shape your organisation's information security strategy. Our consultants have many years of experience working with industry and government, and will help you contextualise the risks identified, offering constructive and pragmatic remediation advice.

We recommend that a debrief conference call is arranged following report delivery, to discuss the technical vulnerabilities, business risks and best course of remediation.

Service Management

We operate a service management process that is integrated with our ISO 9001 Quality Management System.

All projects are assigned a lead consultant and a project manager throughout delivery of the testing. We operate an escalation procedure in the event of unresolved client dissatisfaction; at the time of G-Cloud 15 submission, this procedure has never been used.

Service Constraints and Levels

We do not have service constraints and levels, other than those specifically tailored and agreed in each 'Statement of Work' within a proposal.

Financial Recompense

We do not have a formal recompense model; as part of our ISO 9001 certification and commitment to customer service, we monitor the quality and delivery of all testing services very carefully.

Training

Training is offered in several of the testing service disciplines we offer; we are happy to discuss training options with our customers.

Ordering and Invoicing Process

Our normal process is to produce a 'Statement of Work' within a commercial proposal and once acceptance is given (through a signed order form or purchase order) we will commence the scheduling process.

Fixed price projects are invoiced on acceptance of the deliverables of each work task. Projects undertaken on a time and materials basis are invoiced monthly in arrears. We are happy to discuss the ordering and invoicing process with our customers.

Termination Terms

Refer to the separate 'Terms and Conditions' document.

Data Restoration / Service Migration

Data restoration and service migration is not included in our price.

Customer Responsibilities

All customer responsibilities will be defined in the 'Statement of Work' for each engagement/project.

Technical Requirements

All technical requirements and service dependencies are discussed with the client during scoping, as in most cases each project has different requirements. Technical requirements and testing pre-requisites will be documented in the 'Statement of Work' within the proposal.