Cyber Security
Defence Consultants

Cyber Security Consultancy

May 2024

G-Cloud 14 Service Description

Cyber Security Defence Consultants Limited
St John's Innovation Centre
Cowley Road
Cambridge
CB4 0WS
T: 01223 421577
W: cybersecuritydefence.co.uk

Cloud Security Continuous Risk Assessment – Security Architecture

Cyber Security Defence Consultants

Table of Contents

1 OVERVIEW

Cyber Security Defence Consultants work with organisations to improve and enhance their cybersecurity thresholds. Our teams work within complex and diverse environments to achieve strategic, operational and realistic outcomes, including ISO/IEC27001, Cyber Essentials and Cyber Essentials Plus.

Over multiple consultancy contracts, we have developed and implemented information risk management processes that support our client's governance models and provide support to control specific target areas, improve processes and mitigate risk. This has increased security controls, reducing the organisation's risk appetite and cyber threats.

We engage experienced and qualified consultants who are up to date with all legislative practices to support organisations to manage risk effectively.

Our team holds qualifications including CISSP, CISM and ISO/IEC 27001 Lead Auditor and Lead Implementer.

Our cyber security consultancy engagement process aligns with the NCSC Certified Cyber Security Consultancy Standard, ensuring a high-quality client journey including agreed deliverables, transparent and regular reporting, defined escalation paths, suitably skilled and qualified resources and focused delivery.

2 SERVICE

2.1 Cloud Security Continuous Risk Assessment – Security Architecture

Risk assessment is a tool used to understand all organisational risks on a project.

Cyber Security Defence Consultants provide support and guidance, including managed security services.

We engage CCP Lead and Senior SIRA, Senior Architect Acredditor, and Head Consultant. MITRE ATT&CK framework review and risk assessment methodologies such as ISO 27005, IRAM2, NIST SP800 – 30/53 with experts in supplier assurance, NCSC CAF development and cloud continuous risk assessment, a requirement for secure by design.

Ensuring cloud security is an essential aspect of modern IT infrastructure, and we increasingly work with organisations to secure all controls and mitigate risks.

Elements of the risk security assessment and support that we offer include:

1. **Asset Identification and Valuation**: we identify and classify the organisation's critical assets, such as data, applications, and infrastructure, hosted in the cloud environment. We determine the value and sensitivity of these assets.
2. **Threat Modelling:** analyse all potential threats, including external threats (e.g., cyber-attacks, data breaches) and internal threats (e.g., unauthorised access, insider threats). We consider the likelihood and impact of these threats on the organisation's assets.
3. **Vulnerability Assessment:** conduct vulnerability assessments to identify and prioritise cloud infrastructure, applications, and services vulnerabilities. This can involve penetration testing, code reviews, and configuration audits.
4. **Risk Analysis and Evaluation:** analyse and evaluate the identified risks based on the potential impact and likelihood of occurrence. We prioritise risks and determine appropriate risk treatment strategies (e.g., risk avoidance, mitigation, transfer, or acceptance).

With regards to cloud security architecture, our support includes:

1. **Cloud Security Controls:** implement appropriate security controls based on industry best practices, regulatory requirements, and the organisation's risk appetite. These controls may include access management, data encryption, network security, logging and monitoring, and incident response procedures.

2. **Cloud Service Provider (CSP) Security**: Evaluate the security measures and controls offered by the CSP, including their data centre security, compliance certifications, and shared responsibility model.
3. **Identity and Access Management (IAM):** implement robust IAM mechanisms to manage user identities, roles, and access privileges within the cloud environment. This can sometimes involve integrating with existing identity providers, enforcing multi-factor authentication, and implementing the principle of least privilege.
4. **Data Protection:** implement data protection measures, such as encryption at rest and in transit, key management, and secure data deletion practices. We work with organisations to ensure compliance with data protection regulations, such as GDPR.
5. **Monitoring and logging:** implement robust monitoring and logging mechanisms to promptly detect and respond to security incidents. This can involve integrating with Security Information and Event Management (SIEM) solutions and leveraging cloud-native monitoring tools.
6. **Incident Response and Business Continuity:** develop and maintain an incident response plan and business continuity strategies to ensure the resilience and availability of cloud-based services in the event of security incidents or disasters.

Ongoing security assessment and continuous improvement are also part of this service. This includes:

1. **Continuous Assessment:** regularly assessing and monitoring the cloud environment for any changes in the threat landscape, new vulnerabilities, and evolving security best practices.
2. **Security Automation:** leverage automation tools and scripts to streamline security processes, such as configuration management, vulnerability scanning, and patch management.
3. **Security Awareness and Training:** implement security awareness and training programmes for employees, contractors, and other stakeholders to promote a security-conscious culture.
4. **Compliance and Regulatory Requirements:** ensure compliance with relevant industry regulations, standards, and best practices.

We continually collaborate with organisations and key stakeholders throughout these services to maintain a secure and resilient cloud environment.