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

Third Party Supplier Assurance

Cyber Security Defence Consultants

Table of Contents

1 Overview

Cyber Security Defence Consultants work with organisations to improve and enhance their cybersecurity thresholds.

Over multiple consultancy contracts, we have developed and implemented information risk management processes which support our client's governance models, as well as providing support to control specific target areas, improving processes and mitigating risk. This has increased the level of security controls, ensuring that the risk appetite of the organisation and the level of cyber threat faced is reduced.

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

Our team holds qualifications in line with industry standards including CISSP, CISM and ISO/IEC 27001 Lead Auditor and Lead Implementer.

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

2 Services

2.1 Third Party Supplier Assurance

Cyber Security Defence Consultants provide support to organisations to assess the risks associated with the third-party processes of data. We can advise on governance, technical and organisational controls, and offer remediation guidance for compliance, alongside providing support for existing third-party arrangements and future procurement activity.

The services can offer valuable insights and objective validation, helping organisations to strengthen their cybersecurity defences and build trust with internal and external stakeholders.

Under this service, we can offer:

1. **Cybersecurity Audits and Assessment** – conducting comprehensive evaluations of an organisations cybersecurity controls, policies, procedures, and technologies. They identify potential vulnerabilities, gaps, and areas for improvement, providing recommendations for enhancing the overall security posture.
2. **Penetration Testing and Ethical Hacking** – ethical hackers or penetration testing stimulate real-world cyber-attacks to identify and exploit vulnerabilities in an organisations systems, networks, and applications. This proactive approach helps organisations identify and address security weaknesses before they can be exploited by malicious actors.
3. **Security Compliance Assessments** – third party assessors evaluate an organisation's compliance with relevant cybersecurity standards, regulations, and frameworks, such as Data Protection Act 2018, General Data Protection Regulation, ISO 27001, NIST Cybersecurity Framework, or industry-specific requirements. These assessments provide assurance that the necessary controls and safeguards are in place to meet regulatory and industry requirements.
4. **Vulnerability Assessments and Management** – conducting regular vulnerability assessments to identify and prioritise potential vulnerabilities in an organisation's IT infrastructure, applications, and systems. They may also provide ongoing vulnerability management services, including patch management and remediation guidance.
5. **Security Controls Validation** – we evaluate the design, implementation, and operational effectiveness of an organisation's security controls, such as access controls, encryption, firewalls, and intrusion detection systems, to ensure they are functioning as intended and providing adequate protection.
6. **Cloud-security Assessments** – evaluating the security posture of all cloud environments, including cloud

service provider’s security controls, configuration settings, and compliance with relevant cloud security standards.

7. **Incident Response and Forensic Investigations** – in the event of a cybersecurity incident, our third-party experts can provide incident response services, including forensic analysis, incident containment, and remediation guidance, helping organisations effectively respond to and recover from security breaches.

They provide you with objective and independent evaluations, helping you to identify and mitigate cybersecurity risks, demonstrate compliance, and build trust with customers, partners, and regulatory bodies.