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

Managed Security Service – SbD (Secure by Design)

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 hold 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 Services

2.1 Managed Security Service – SbD (Secure by Design)

Cyber Security Defence Consultants offer ongoing information security management to ensure all information assets are appropriately protected and that legal and regulatory compliance requirements are met. Our solutions ensure robust risk management, security control implementation, and continuous lifecycle support, aligning with NCSC guidelines and NIST security standards for public sector outcomes. It is ideal for projects demanding robust, repeatable security integration.

This includes:

1. Security delivered in parallel with the design of the solution/architecture
2. Risk Assessments to identify risks faced by each organisation
3. Consultancy on securing systems and services
4. Gap analysis, auditing, and full compliance with recognised security standards, such as ISO27001.
5. Security incident prevention and management
6. Advise on or produce a business case for introducing security controls.
7. Cyber secure design services for the public sector, experts in AWS and Azure
8. Define security requirements early in the project lifecycle and risk and threat assessment.
9. Utilise defence layers and secure architectures to deliver the design effectively.
10. Implementing continuous risk assessment and management in the cloud
11. Security control implementation and testing, Experienced and qualified security professionals
12. Ensure security mitigations are scalable and reusable and have a cost-effective security design.
13. Security controls based on identified risk, maturing cloud security posture.
14. Validate and verify security measures at design points security testing.
15. Service suitable for Public, Community, Hybrid and Private Cloud
16. Vendor-agnostic supplier providing unbiased independent advice.

Service benefits include:

1. Highly experienced UK-based consultants
2. Experienced security testing and assurance teams with comprehensive, varied experience
3. As independent information security specialists, we provide unbiased services
4. Advice and recommendations are given with a genuinely holistic security view

5. All deliverables are independently quality-assured and reviewed.
6. Increased compliance whilst reducing risks to reputation damage

This service helps organisations offload the operational burden of security monitoring and management, using risk assessments to identify and prioritise security risks.

With this, we work with organisations to establish a robust cybersecurity posture, enabling them to proactively identify and mitigate risks, respond to security incidents, and comply with relevant regulations and industry standards.