Cyber Security
Defence Consultants

Cyber Security Consultancy

January 2026

G-Cloud 15 Service Description

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

Azure Cloud Security Architecture Review

Cyber Security Defence Consultants

Table of Contents

Service Definition Document

Azure Cloud Security Architecture Review

1 Overview

Cyber Security Defence Consultants delivers comprehensive Microsoft Azure cloud security architecture reviews for UK government departments and public sector organisations.

Our consultants assess Azure environments against the Azure Well-Architected Framework security pillar and NCSC cloud security principles, identifying misconfigurations, security gaps, and opportunities for improvement. We deliver practical, prioritised recommendations that balance security requirements with operational needs.

All consultants hold SC clearance and relevant professional certifications including Azure Security Engineer Associate, CISSP, and CISM. Our team has direct experience securing Azure environments for central government departments including Entra ID implementations and Conditional Access deployments.

2 Service Description

2.1 Assessment Scope

Our Azure security architecture review covers the following domains:

2.1.1 Identity and Access Management

- Entra ID (Azure AD) configuration and tenant security
- Conditional Access policies and authentication methods
- Privileged Identity Management (PIM) configuration
- Role-based access control (RBAC) assignments

2.1.2 Network Security

- Virtual network architecture and segmentation
- Network Security Groups and Application Security Groups
- Azure Firewall and Web Application Firewall configurations
- Private endpoints and service endpoints

2.1.3 Data Protection

- Encryption at rest and in transit configurations
- Azure Key Vault management and access policies
- Storage account security and access controls
- Microsoft Purview data classification integration

2.1.4 Security Monitoring

- Microsoft Defender for Cloud configuration and coverage
- Microsoft Sentinel deployment and analytics rules
- Activity logs and diagnostic settings
- Alert configuration and incident response integration

3 Key Features

1. Entra ID configuration review including Conditional Access policies
2. Network security assessment covering VNets, NSGs, and Azure Firewall
3. Data protection review including encryption and Key Vault management
4. Microsoft Defender for Cloud configuration and recommendations analysis
5. Azure Well-Architected Framework security pillar alignment
6. NCSC cloud security principles compliance assessment
7. Management group and subscription security review
8. Azure Policy and compliance assessment
9. Prioritised remediation roadmap with implementation guidance
10. Executive summary and technical findings report

4 Key Benefits

11. Identifies security misconfigurations before they become incidents
12. Provides clear prioritised remediation roadmap
13. Aligns Azure environment with government security requirements
14. Reduces attack surface through configuration improvements
15. Demonstrates security due diligence to stakeholders
16. Supports compliance with NCSC cloud security guidance
17. Transfers knowledge to internal teams during engagement
18. Validates existing security controls against best practice
19. Optimises Microsoft Defender for Cloud security posture score
20. Delivered by SC-cleared consultants with Azure experience

5 Pricing

Services are delivered on a time and materials basis using SFIA day rates. Rates range from £500 to £1,150 per day depending on consultant seniority (SFIA Levels 1-7). Fixed price engagements available for defined scope assessments.

Travel and subsistence within M25 included. Outside M25 charged at departmental rates. See separate Pricing Document and SFIA Rate Card for full details.

6 Support

Standard Support (included): Pre-engagement scoping, dedicated assessor contact throughout engagement, post-engagement support for 30 days including report clarification and remediation guidance.

Enhanced Support (additional cost): Extended support, annual reassessments, ongoing maturity tracking. Available at SFIA day rates.

Response Times: Initial response within 4 business hours during UK business hours (09:00-17:00 Monday to Friday). Urgent matters escalated immediately.

7 QUALIFICATIONS AND CERTIFICATIONS

- All assessors hold Security Clearance (SC)
- Staff screening to BS7858:2019
- Cyber Essentials Plus certified
- Professional certifications: CISSP, CISM, ISO 27001 Lead Auditor/Implementer
- Engagement process aligned to NCSC Certified Cyber Security Consultancy Standard