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

Incident Response Planning and Tabletop Exercises

Cyber Security Defence Consultants

Table of Contents

Service Definition Document

Incident Response Planning and Tabletop Exercises

1 Overview

Cyber Security Defence Consultants delivers incident response planning and tabletop exercise services designed to prepare UK government and public sector organisations for cyber security incidents. Our services help organisations develop, document, and test their incident response capabilities in a safe, controlled environment.

Effective incident response requires more than documentation—it requires practiced, coordinated action across technical teams, management, and leadership. Our tabletop exercises create realistic scenarios that test decision-making, communication, and coordination before real incidents occur.

All services are delivered by SC-cleared consultants with extensive experience in cyber incident response across government and critical national infrastructure sector.

1 Service Components

2.1 Incident Response Plan Development

We develop comprehensive incident response plans aligned to NCSC guidance and your organisation's specific requirements:

- Incident classification and severity frameworks
- Roles, responsibilities, and escalation procedures
- Detection, containment, eradication, and recovery procedures
- Internal and external communication plans
- Integration with business continuity arrangements
- Post-incident review and lessons learned processes

2.2 Tabletop Exercise

Facilitated discussion-based exercises that walk participants through realistic cyber incident scenarios:

- Customised scenarios based on your threat landscape and risk profile
- Ransomware, data breach, insider threat, and supply chain scenarios
- Facilitation by experienced incident response practitioners
- Injects that evolve the scenario and test escalation decisions
- Structured debrief identifying strengths and improvement areas

2.3 Crisis Simulations

More intensive exercises for senior leadership teams focusing on strategic decision-making:

- Board-level crisis management exercises
- Media and stakeholder communication scenarios
- Regulatory notification decision-making
- Business impact and recovery prioritisation
- Cross-functional coordination testing

3 GovAssure and CAF Alignment

Our services directly support GovAssure compliance, particularly CAF Objective D (Minimising the Impact of Cyber Security Incidents):

- **D1 Response and Recovery Planning:** Documented, tested incident response plans
- **D2 Lessons Learned:** Post-exercise review and improvement processes
- Evidence of exercised plans for GovAssure assessments

4 Typical Engagement

4.1 Tabletop Exercise Package (5-8 days)

1. **Scoping and Planning (1-2 days):** Review existing plans, understand threat landscape, identify participants
2. **Scenario Development (1-2 days):** Create realistic scenario with timed injects and decision points
3. **Exercise Delivery (1 day):** Facilitated 3-4 hour exercise with key stakeholders
4. **Debrief and Reporting (2 days):** Structured debrief, findings analysis, improvement recommendations

4.2 Full Incident Response Programme (15-25 days)

- Incident response plan development or review
- Playbook creation for priority incident types
- Communication plan development
- Multiple tabletop exercises across different scenarios
- Training delivery for incident response team

5 PRICING

Services are priced based on SFIA day rates. See separate Pricing Document for full rate card.

- SFIA Level 4 (Senior Practitioner): £500/day
- SFIA Level 5 (Senior Consultant): £700/day
- SFIA Level 6 (Principal Consultant): £900/day
- SFIA Level 7 (Lead Consultant): £1,150/day
- Working day: 7.5 hours

Typical tabletop exercise package (5-8 days): £3,500 - £6,400 depending on complexity and consultant level.

6 SUPPORT

Standard Support (included): Named SC-cleared analyst, UK business hours monitoring, monthly reports, policy changes within 2 working days, quarterly reviews.

Enhanced Support (additional cost): Extended hours, priority response, dedicated TAM, custom reporting.

Response Times: 4 business hours initial response. Critical security incidents 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