Cyberfort

G-Cloud 15

Service Definition

Security Testing Services

Table of Contents

1. Service Overview

Cyberfort are an NCSC-Assured Service Provider, accredited by CREST and CHECK for Penetration Testing, Vulnerability Scanning and Cyber Essentials assessments, with 100% success rate. Our testers hold CHECK, CREST, and OSCP certifications, combining technical depth with experience of GovAssure, CAF, and Secure-by-Design (SbD) programmes.

Cyberfort's approach to Security Testing is designed to identify, validate, and help remediate security vulnerabilities across infrastructure, cloud, applications, and endpoints. Our methodology is rooted in NCSC best practice, CHECK and CREST governance, and industry standard testing techniques, ensuring assessments are safe, repeatable, and technically rigorous.

We adopt a hybrid testing model, combining expert-led manual penetration testing with automated tools, to deliver depth, breadth, and high assurance. This enables us to uncover complex weaknesses including chained exploits, business logic flaws, misconfigurations, and zero-day type exposures that traditional scanning alone cannot identify.

Cyberfort's testing methodology consistently delivers high-value insights by assessing your environment through the lens of a real threat actor, while providing structured risk reduction aligned with UK government and regulatory expectations.

1.1 Our Approach to Security Testing

Our approach recognises that client systems must remain available, stable, and secure at all times. Therefore, Cyberfort implements a comprehensive assurance framework to ensure continuity of service throughout the entire testing lifecycle, from scoping to execution, reporting, and closure.

We follow a structured, standards-led approach to ensure all testing is delivered safely, efficiently, and fully aligned with clients' requirements.

1.1.1 End-to-End Testing Delivery Model

Cyberfort follows a structured delivery framework:

Stage	KPI/SLA	Milestone / Output
Scope Request Received	<4 working hours	Formal receipt of client request and validation of required testing services.
Scoping Meeting & Risk Assessment	<3 working days of request	Collaborative scoping session to define testing boundaries, operational constraints, asset lists, data sensitivity, test windows, and escalation routes.
Statement of Work (SoW)	<3 working days of scoping meeting	Delivery of the SoW, risk register, documentation, and readiness assessment for formal approval.
Client Authorisation	Client dependant	Client confirms acceptance of SoW and provides authorisation for testing. Formal readiness confirmation issued.
Testing Delivery	Scope specific timelines	Execution by CHECK/CREST-certified testers using safe, controlled methodologies aligned with NCSC standards.

		Testing timescales are varied and dependent on the scope of testing, on average testing windows range from 2 to 8 weeks.
Initial Report	Ongoing through testing Phase	Real-time documentation, daily internal QA, draft reporting begins concurrently with testing.
Final Test Report	<5 working days of test completion	Full written report of all findings in accordance with NCSC CHECK scheme guidelines.
Post-test meeting/ de-brief	<5 working days of test completion	Final report delivery, technical and executive summary walk-throughs, remediation Q&A sessions.
Continuous Support & Retesting	As agreed with client	Ongoing technical support, remediation guidance, and optional retesting to validate fixes.

This end-to-end structure ensures predictable delivery, controlled risk, and consistent documentation.

1.1.2 Collaborative Scoping to Minimise Operational Impact

The scoping process defines objectives, boundaries, constraints, and authorisation protocols to minimise disruption and maximise value. Recognising each engagement is unique, we will work closely with client teams to meet objectives, timelines, and compliance needs.

We will conduct detailed scoping and risk assessment, including:

- **Assets and Systems:** IP ranges, hostnames, web applications, cloud tenants, mobile apps, and internal subnets.
- **Testing Boundaries:** Defined attack surfaces, user roles, and privilege levels.
- **Testing Depth:** Level of testing (black box, grey box, white box).
- **Constraints:** Maintenance windows, critical system exclusions, or test restrictions agreed with client.

This approach ensures testing efforts align directly to clients risk tolerance, business criticality, and security maturity.

1.1.3 Governance and Sign-Off

Governance ensures every engagement meets internal and client-specific controls:

- **Internal Governance Review:** QA Reviewer validates the scope, tooling, authorisation, and resource allocation.
- **Formal Authority Sign-Off:** Authority provides written approval before any testing commences.
- **Change Control:** Any amendments to scope or timeline require formal approval via Change Request Form.
- **Pre-Delivery Readiness Checklist:** Confirming approvals, access credentials, and communications plan prior to commencement.

All sign-off points are recorded and retained as part of Cyberfort's Quality Management System.

1.1.4 Risk Management Considerations

Cyberfort applies a Risk-Based Testing Framework, aligned with ISO:31000 and NCSC best practice. Key principles include:

- Pre-engagement risk assessment to evaluate service impact and operational dependencies.
- Authorisation controls to ensure client's awareness of testing risks (e.g., potential performance impact).
- Controlled testing windows with rollback procedures for critical systems.
- Contingency and escalation procedures, including emergency stop protocols and incident notification paths.
- Post-test assurance confirming no residual system degradation.

1.1.5 Communication and Documentation

All client interactions are documented and centrally stored in Cyberfort's ISO:27001-certified information management system. Outputs include:

- **Statement of Works (SoW):** Detailing test objectives, scope boundaries, and risk mitigations.
- **Authorisation Form:** Signed by both parties before commencement.
- **Engagement Plan:** Including testing schedule, escalation matrix, and communication cadence.
- **Risk Register:** Maintained throughout the engagement lifecycle.

Cyberfort uses encrypted email, secure SharePoint, or the Cyberfort Client Portal for all document exchanges. Reports and communications are version-controlled and auditable.

1.1.6 Lead Time and Mobilisation

Cyberfort has a mature, structured mobilisation process that enables rapid commencement of testing following receipt of a confirmed scope. We offer two mobilisation pathways depending on the urgency and business requirements:

Mobilisation Type	Lead Time	Description
Standard Mobilisation	Within 5 working days	For routine engagements with defined scope and authorisation.
Accelerated Mobilisation	Within 48 hours	Reserved for high-priority or time-sensitive requests, subject to system access and risk approval.

These SLAs are supported by our permanent in-house pool of CHECK Team Leaders (CTLs), Security Consultants, and CREST-certified penetration testers, enabling flexible, reliable scheduling across the contract term.

1.1.7 Typical Testing Phases

During scoping, we work with our clients to define realistic, mutually agreed timelines aligned with requirements. The below details typical steps in our penetration testing engagements against a standard IT Health Check of 1000 seats.

Testing Phase	Steps
Information Gathering	DNS enumeration, open-source intelligence (OSINT), and foot printing to identify attack surfaces.
Vulnerability Assessment & Exploitation	Using combination of automated-scanners and manual inspection to locate weaknesses. Safely exploiting vulnerabilities to determine potential business impact and validate findings.
Privilege Escalation & Lateral Movement	Assessing internal pivoting opportunities post-compromise.
Post-Exploitation & Data Validation	Verifying data sensitivity and testing resilience measures.
Reporting & Debrief	Consolidating findings, impact analysis, and remediation guidance.
Remediation Support and Follow-up	Provide guidance and support during remediation to help your team understand and fix vulnerabilities, followed by re-testing to confirm they have been resolved.

Our testing approach is controlled and authorised, ensuring that all activities are logged, reversible, and aligned with client's operational continuity requirements.

1.1.8 Secure Remote Testing Setup

All remote testing is executed by Cyberfort UK-based, SC cleared, CHECK-certified testers in secured UK environments that comply with clients's requirements.

Controls and Protocols

- Testing devices hardened to NCSC configuration standards.
- Connectivity via client-approved VPNs and secure access protocols.
- No data processed or stored outside the UK.
- Day-one validation of connectivity and logging to ensure traceable access.
- All access will be logged and monitored, and any deviations will be escalated to the Service Owners.

1.1.9 Test Reporting

Cyberfort's reporting is built on five key principles:

1. **Clarity** Findings expressed in plain English.
2. **Accuracy** Every finding manually verified, peer-reviewed, and validated.
3. **Relevance** Reports tailored to client's environment, risk appetite, and audience.
4. **Actionability** Each recommendation prioritised and aligned to business objectives.
5. **Assurance** Findings supported by evidence, governance sign-off, and defensible methodologies.

This ensures reports are not merely technical outputs but strategic tools for improving resilience and compliance.

1.1.10 Content Structure and Reporting Detail

Each Cyberfort report follows a consistent, well-defined structure:

Executive Summary

Introduction	Overview of engagement type, objectives, and systems tested.
Methodology	Standards and testing methods applied.
Summary of Findings	Aggregated results by severity, with risk distribution charts.
Business Impact Analysis	Contextual explanation of potential operational or reputational impact.
Key Recommendations	Prioritised actions for remediation and strategic improvement.
Next Steps	Outline of proposed follow-up testing or support.

Technical Findings

Vulnerability Overview	Categorised by asset, risk rating, and CVSS score.
Detailed Findings	Vulnerability description and affected components. Evidence (screenshots, logs, exploit output). Proof of concept (where safe and permitted). Remediation steps with vendor references. Residual risk and likelihood of recurrence.
Appendices	Tool versions, configurations, and test parameters for audit traceability.

1.1.11 Governance and Quality Assurance

Every report undergoes a three-stage governance process:

1. **Technical Review:** Validation to ensure technical accuracy and alignment with CHECK/NCSC standards.
2. **Quality Assurance Review:** Independent evaluation by the QA Reviewer to confirm findings are verified, risk-rated, and clearly articulated.
3. **Management Approval:** Head of Offensive Security confirms alignment with standards and contractual commitments.

1.1.12 Post-Engagement Workflow

Cyberfort recognises that the true value of Penetration Testing and ITHC's lies not only in the identification of vulnerabilities but in the clear communication of results, guidance for remediation, and verification of closure.

Our Post Testing service provides clients with a structured, transparent process that ensures:

- Findings are clearly communicated and understood.
- Actionable remediation guidance is provided.
- Retesting and verification are conducted effectively.
- False positives are eliminated, and closure is formally confirmed.

Cyberfort follows a consistent and auditable process after every engagement to ensure complete service closure:

Phase	Activity	Deliverable / Outcome
1. Completion Confirmation	Validate that testing/scanning has concluded safely and systems are stable.	Completion Certificate and readiness for reporting.
2. Reporting & Communication	Deliver and explain findings to Authority stakeholders.	Executive and Technical Reports.
3. Remediation Support	Provide clear guidance on corrective actions and risk prioritisation.	Remediation Plan / Vulnerability Register.
4. Retesting & Verification	Validate implementation of remediation activities.	Retest Report and updated risk profile.
5. Closure & Governance Sign-Off	Confirm resolution of all findings, including false positives.	Closure Certificate / Final Authority sign-off.

2. Our Experience

Our clients range from the largest of HMG departments, to non-departmental public bodies including projects of critical national infrastructure status. Our private sector work is equally wide-ranging, including blue-chip and FTSE companies, SMEs and agile technology start-ups.

Case Study – HMG Central Government Department

THE CHALLENGE

The customer uses multiple complex applications that hold sensitive and regulated data. Upholding the accessibility, integrity and privacy of this data is mandatory. The customer required expertise in testing and verifying the security controls of the applications and supporting infrastructure.

THE SOLUTION

Cyberfort have provided CHECK ITHC Penetration Testing and security reviews on multiple applications testing.

In collaboration with the customer development team, Cyberfort delivered a straightforward, effective approach that surpassed mere adherence to compliance norms. We invested significant time to thoroughly comprehend the application's functions and structure, which allowed us to identify potential attack points and vulnerabilities, as well as their possible business consequences.

Our contribution was instrumental in creating comprehensive and understandable reports, providing both the technical team and the executive suite with the necessary data to bolster the overall security posture.

THE OUTCOME

Our versatile approach leaves no stone unturned, benefiting customer and their diverse range of clients by ensuring that their applications undergo thorough testing according to the highest industry standards. By providing clear, well-written reports with actionable steps, Cyberfort enables the customer to promptly address vulnerabilities, resulting in reduced development cycles, adherence to launch schedules, and meeting customer expectations across various applications.

SOLUTION PROVIDED

- CHECK ITHC Penetration Testing Code Reviews
- Threat Modelling
- Remediation Roadmap
- Secure Code Review

BUSINESS RESULTS

- Enhanced security of applications and infrastructure.
- Go-Live targets achieved.
- Brand protection.
- Compliance.
- Improved SDLC
- Actionable plan for the next 12mths.

3. Commercials & Pricing

3.1 Ordering & Invoicing Process

Please contact us for a quote via email at bidmanagement@cyberfortgroup.com

Orders are processed on receipt of a purchase order.

Prior to commencement of any work ordered via the G-Cloud framework, Cyberfort requires client acceptance of the order and also completion of a Call-Off Contract.

Clients are invoiced on a monthly basis or according to agreed milestones.

3.2 Service pricing model

Cyberfort's pricing for Security Testing links clearly to Resources Based Pricing detailed in our SFIA rate card framework.

Please refer to our Pricing document for more details.

3.3 Minimum contract period

Contract terms will be provided at the time of quotation, based on specification. These will not exceed the maximum contract constraints of the G-Cloud framework.

4. Governance Compliance

Cyberfort confirm that we will deliver our services to clients in line with all industry and Government recognised standards, best practice and legal regulations, including but not limited to the following:

4.1 GDPR

We adhere to the legal and statutory requirements outlined in the UK Data Protection Act 2018 and the General Data Protection Regulations (GDPR). Our organisation has a current registered Information Commissioners Office (ICO) certificate for Data Protection.

4.2 Government and industry standards

Throughout the life of any contract, our consultants will ensure that all service standard principles are adhered to so that clients can be assured that all delivered outcomes conform with Government and industry standards and expectations. Our teams are deeply experienced in operating services, to deliver outcomes and outputs that fully comply with:

- The principles defined in the Government's Service Standard and Technology Code of Practice (TCoP).
- The Government Functional Standard (GovS 007: Security), ensuring that the stated principles (for example security objectives are aligned to government policy and organisational objectives) are applied to all projects.
- Open standards supported include TOGAF, NIST-CSF, ISO/IEC27000, SANS and OWASP.
- Regulation frameworks including, Cyber Security and Resilience Bill, Digital Operational Resilience Act (DORA), and NIS2 Directive.
- Government Cyber Security Strategy, including National Cyber Security Centre (NCSC).
- As an NCSC assured Cyber Security Consultancy, we are members of the NCSC Assured Consultancy Scheme Community Network and leverage the CiSP (Cyber Information Sharing) platform.

4.3 Quality Management

Further, we have a fully implemented Quality Management System (QMS) and are certified to ISO 9001:2015 International Standard, which details our policy, objectives and processes, as well as demonstrating how our QMS framework enhances client satisfaction whilst ensuring consistent delivery of product and services is maintained to meet client, statutory and regulatory requirements.

Our delivery is underpinned by certifications and associated management systems including:

- ISO:27001
- ISO:14001
- ISO:9001
- ISO:45001
- Cyber Essentials Plus
- CREST Certified Body CE
- CREST Penetration testing
- NHS Digital Toolbox
- PCI DSS
- DSPT
- NCSC Cyber Security Consultancy
- NCSC CHECK ITHC

About Cyberfort

Cyberfort's all-encompassing Cyber Security Services

At Cyberfort we provide a range of customers with all-encompassing Cyber Security Services. We are passionate about the cyber security services we deliver for our customers which keeps their people, data, systems and technology infrastructure secure, resilient and compliant.

Our business offers National Cyber Security Centre assured Consultancy services, Identification and Protection against cyber-attacks, proactive Detection and Response to security incidents through our security operations centre and a Secure and Recover set of Cloud solutions which keeps data safely stored, managed and available 24/7/365.

Over the past 20 years we have combined our market leading accreditations, peerless cyber security expertise, strong technology partnerships, investment in our future cyber professionals and secure locations to deliver a cyber security experience for customers which enables them to achieve their business and technology goals in an ever-changing digital world.

Cyberfort

Care about the impacts we make on the Environment, Social and Governance.

We are passionate about empowering our employees, suppliers, customers, and the cyber security ecosystem to create a better world for our business and the communities we participate in, for example:

As a member of Neurodiversity in Business (NiB) and Disability Confident Employer

Cyberfort are supporting those with physical and neurodiverse disabilities, by disarming barriers for people with disabilities and ensuring equal opportunities for all.

Cyberfort are inspiring and attracting young people to the world of cybersecurity.

We support the development of their passion for technology through Apprenticeships, Graduate Schemes, CyberFirst and school education/awareness.

We are committed to achieving net zero carbon emissions by 2050.

Cyberfort have clear plans and activities that deliver environmental benefits by increasing the energy efficiency of our operations, reduce our waste, and protect our communities.

Our Values

Teamwork | Curiosity

Ownership | Agile | Innovative

Cyberfort

Accreditations

We are proud of the extensive list of industry and government accreditations we hold. We understand the need for independent validation when entrusting the security of valuable or sensitive data to a third party.

Our Vision

To be an integral part of the cyber security ecosystem, providing assured, highly skilled and reliable security services to businesses and government departments. Embodying the UK Cyber Security Strategy, through trusted partnerships we aim to empower businesses and government departments with confidence, making the world a safe and secure place to conduct business.

Our Mission

To provide our customers with an agile and innovative approach to help them overcome their cyber security challenges. Through a collaborative approach with our customers we design, build and operate their cyber security environments resulting in a secure and resilient infrastructure, providing a safe environment for employees, service users and stakeholders to conduct their business in the knowledge that their critical data remains safe in an ever-changing digital world.

www.cyberfortgroup.com

For more information, please contact us on:

01304 814800

info@cyberfortgroup.com