NCSC IT Health Check

G-Could-15

Service Definition Document

2026-01-16

REVERSEC

28 January 2026

1 NCSC IT Health Check

Led, managed and delivered by our specialist CHECK & CREST dual certified personnel (Infrastructure and Application); utilising a proven methodology refined over many years of CHECK testing, providing coverage of all operating systems and applications. Includes vulnerability scanning and manual analysis of organisations' internal and external network.

1.1 Service scope

This service delivers an NCSC CHECK-approved assessment to identify security weaknesses across in-scope systems through independent, expert technical testing. Activities may include external and internal penetration testing, application testing, configuration and build reviews, and firewall or network rule audits, depending on the agreed scope. The objective is to detect vulnerabilities and configuration flaws, assess exposure to realistic threats, and provide risk-prioritised remediation guidance. All testing is performed by CHECK-certified personnel in accordance with NCSC's IT Health Check requirements.

1.2 Service features and benefits

1.2.1 Service features

- Desktop / server build and configuration.
- Network management security review.
- Analysis of patching at OS, application and firmware level.
- Configuration review of remote access solutions (managed-devices and BYOD).
- Build and configuration reviews of laptops / mobile devices.
- Internal security gateway configuration (including PSN gateway) assessment.
- Wireless network configuration analysis.

1.2.2 Service benefits

- Ensure external systems are protected from unauthorised access / change.
- Ensures absence of unauthorised entry points that consume PSN services.
- Detailed and comprehensive report with mitigation recommendations.
- Risks relating to exploitation identified and remediation recommendations provided.

1.3 Support

Standard project support is provided via email, phone, and optional secure chat—each available Monday to Friday, 9am–5pm (UK time). Additional Support provision can be agreed per project which may incur an additional charge (please see price list).

1.4 Staff security

Staff are screened to BS7858:2019 standards, with personnel eligible for UK Government security clearances up to Developed Vetting (DV)

1.5 Project Management

Contracting with Reversec provides our client with a fully managed project planning and delivery process. To oversee the successful delivery of each engagement, Reversec shall assign an Engagement Lead for the duration of the engagement. Reversec Engagement Managers have various qualifications including PMP, AGILE, PRINCE2 and/or ITIL and follow industry best practices that can be aligned to match Our client preferred internal project management practices. The allocated Engagement Lead will also have relevant experience of delivering similar projects to global organizations across different industries and be able to proactively advise on delivery execution options.

1.6 Communication

Reversec provides a dedicated engagement manager as the primary contact during business hours, with immediate alerts for critical vulnerabilities. Clear, secure communication channels support real-time collaboration, while a structured communication plan ensures stakeholders receive timely, accurate, and actionable updates throughout the engagement

1.7 Quality Assurance

Reversec has been successfully assessed against the Council of Registered Ethical Security Testers (CREST) criteria for the ethical practice and supply of advanced cyber services; CREST regulations form a critical part of Reversec's own quality management processes and have informed the internal governance process.

1.8 Information Security

Our organization is committed to maintaining the highest standards of information security, in line with industry's best practices and regulatory requirements. As an ISO/IEC 27001:2022 certified company, we operate a comprehensive Information Security.

CLIENT CONFIDENTIAL