

Network Security Assurance

GG-Could-15

Service Definition Document

2026-01-16

1 Network Security Assurance

Network security assurance enables organisations to determine whether exploitable vulnerabilities exist on the organisation's internal or external network infrastructure that would enable an attacker to gain access to high-value systems and applications.

1.1 Service scope

This service assesses the security of on-premises, cloud, and hybrid networks to identify exploitable weaknesses. It reviews network architecture, segmentation, perimeter controls, firewall and IPS/WAF policies, remote access solutions, wireless security, routing, DNS/DHCP hygiene, and cloud networking configurations. Device hardening and logging/monitoring coverage are evaluated to ensure effective detection and response. Where needed, authenticated configuration reviews and targeted network penetration testing validate real-world exploitability and lateral-movement risk. Deliverables include a risk-prioritised report, annotated network diagrams, hardening actions, architectural recommendations, and a remediation retest window, aligned with recognised good practice and suitable for governance and audit.

1.2 Service features and benefits

1.2.1 Service features

- Penetration testing of environments
- Prioritised guidance for improving overall network security
- Goal-based assessments to identify business risks
- Review components in the context of the wider infrastructure layout

1.2.2 Service benefits

- Develops an organisation's understanding of network segments and linked components
- Overlaps with the assessment of key applications determining broader risk
- Provides understanding of organisations' security postures and identifies key vulnerabilities
- Provides remediation advice of how to address vulnerabilities at root-cause

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 Reversesec provides our client with a fully managed project planning and delivery process. To oversee the successful delivery of each engagement, Reversesec shall assign an Engagement Lead for the duration of the engagement. Reversesec 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

Reversesec 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

Reversesec 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 Reversesec'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.