

Active Directory Security Reviews

G-Could-15

Service Definition Document

2026-01-28

1 Active Directory Service Review

An Active Directory Service Review (ADSR) gives you deep insight into the health, security, and efficiency of your identity environment. By uncovering misconfigurations, strengthening access controls, and validating best-practice alignment, it ensures a resilient foundation for your organisation. Gain clarity, reduce risk, and optimise Active Directory for long-term stability and security.

1.1 Service scope

This service provides a comprehensive evaluation of an organisation's Active Directory configuration, security posture, operational health, and alignment with best practice. It includes review of domain architecture, access rights, group policy, authentication controls, delegation, replication, and identity-related risks. Deliverables include a detailed assessment report, prioritised remediation actions, and recommendations to stabilise, secure, and optimise the AD environment.

1.2 Service features and benefits

1.2.1 Service features

- Simulates targeted cyberattacks across multiple stages of the kill chain
- Proprietary tooling replicates up to 1,000 attacker techniques
- Assesses detection and response capabilities end-to-end
- Provides actionable recommendations for people, process, and technology
- Customisable engagements aligned to organisational threat profiles

1.2.2 Service benefits

- Accelerate risk reduction by identifying and remediating weaknesses
- Improves detection and response timeliness to minimise breach impact
- Strengthens overall security posture through defence-in-depth assessment
- Reduces long-term security costs via proactive improvements
- Supports compliance with industry standards and frameworks

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