

Application Security Assurance

GG-Could-15

Service Definition Document

2026-01-16

1 Application Security Assurance

Application Security Assurance is designed to assess digital applications against “known” vulnerability types (such as those recorded in the OWASP Top 10) to identify exploitable vulnerabilities which could be leveraged by a malicious actor. This level of assessment goes beyond signature-based scanning activities providing increased assurance and resilience to attack.

1.1 Service scope

This service assesses the security of web, mobile, and API-based applications across their lifecycle to identify vulnerabilities, misconfigurations, and design weaknesses before exploitation. It includes threat modelling, secure design review, dependency and SBOM analysis, static/dynamic testing (SAST/DAST), API and authentication/authorisation evaluation, configuration and secrets hygiene checks, and secure deployment pipeline review (CI/CD). Where applicable, it incorporates manual penetration testing to validate findings and exploit paths with business-impact context. Deliverables include a risk-prioritised report, developer-ready remediation guidance with code-level examples, an assurance statement suitable for governance and audit, and a retest window to confirm fixes. The service aligns with recognised good practice (e.g., OWASP ASVS/Top 10, MASVS) and can be delivered as a one-off engagement or as a recurring assurance cadence integrated with release cycles.

1.2 Service features and benefits

1.2.1 Service features

- Penetration testing of internal and external applications
- Ensures that users are only able to perform intended actions
- Ensures that attacker ability to abuse compromise accounts is limited
- Accurately simulates capable threat actor groups and sophisticated techniques
- Uses Reversesec’s consultancy expertise in responding to real-world cyber incidents

1.2.2 Service benefits

- Replicates advanced attacker Tactics, Techniques and Procedures (TTPs)
- Applies pragmatic, goal-focused approaches, ensuring testing time is utilised optimally
- Identifies vulnerabilities with reference to impact
- Incorporates broader business awareness to ascertain broader implications of compromise
- Identifies root-cause to generate wider improvements

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.