ITNextGen Limited
Digital Technology Specialists

G-Cloud 15 Service Definition Document

Security Testing Service

ITNextGen Limited

E: publicsector@itnextgen.co.uk | M: 07545809681 | W: www.itnextgen.co.uk

Service Overview

ITNextGen's Security Testing Services provide ethical hackers and security testers who identify vulnerabilities in public sector applications, infrastructure, and networks. We conduct penetration testing, vulnerability assessments, and security code reviews ensuring government systems meet NCSC guidance, Cyber Essentials Plus, and industry security standards.

Service Description

Our consultants perform comprehensive security testing including web application testing (OWASP Top 10), infrastructure testing, API security testing, and cloud security assessments. We use manual testing techniques and automated tools (Burp Suite, OWASP ZAP, Nessus), providing detailed findings with remediation guidance. All testing follows CHECK scheme principles and government security testing protocols.

Service Benefits

- Identified vulnerabilities before attackers exploit them in production
- Improved security posture through comprehensive vulnerability assessment coverage
- Reduced breach risk with proactive security testing and remediation
- Better compliance with NCSC, Cyber Essentials Plus standards
- Enhanced stakeholder confidence through independent security validation reports
- Lower remediation costs via early vulnerability detection and fixes
- Strengthened security awareness through detailed findings and training

Service Features

- UK-based security testers with CHECK team member certifications
- OWASP Top 10 testing for web applications and APIs
- Infrastructure penetration testing across networks and cloud platforms
- Security code review using SAST tools and manual analysis
- Cloud security assessment for AWS, Azure, and GCP
- Social engineering and phishing simulation testing capabilities
- SC/DV cleared consultants for sensitive government security assessments

Service Scope

The service covers security test planning, reconnaissance, vulnerability scanning, exploitation testing, privilege escalation testing, and reporting with remediation guidance. We specialise in web application testing, API testing, infrastructure testing, wireless testing, mobile application testing, and cloud security assessments. Re-testing validates fixes.

Deliverables

Typical deliverables include security test plans, vulnerability assessment reports, penetration test reports, executive summaries, technical findings with CVSS scoring, proof-of-concept exploits, remediation roadmaps, re-test validation reports, and security awareness materials. All reports follow NCSC reporting standards and government classification requirements.

Onboarding and Offboarding

At service initiation, ITNextGen agrees scope, roles, SFIA levels, delivery approach, and reporting cadence with the buyer. Consultants are onboarded in line with buyer security and access processes. On completion, structured handover and knowledge transfer are provided, and access to buyer systems is removed in accordance with agreed offboarding procedures.

Security and Compliance

The service operates in alignment with ISO/IEC 27001 information security principles and UK government cloud security guidance. Consultants follow role-based access controls, least-privilege principles, secure change management, and incident reporting processes. Where required, consultants may be SC/DV eligible and comply with buyer-specific security requirements.

Service Constraints

Delivery is UK-based and remote-first; on-site engagement is available by agreement. Buyer access to relevant systems, environments, and data is required. Use of specific tools or platforms may require buyer-provided licences. Performance depends on timely buyer feedback, approvals, and access to subject matter experts.

Exit Management

At the end of the engagement, ITNextGen provides agreed deliverables, documentation, and knowledge transfer. All access to buyer systems is removed in line with buyer offboarding policies and contractual requirements.