GlobalLogic®
A Hitachi Group Company

GlobalLogic Security Testing: Penetration, SAST, DAST, Container & Supply Chain Security

SERVICE DEFINITION DOCUMENT - VERSION 1.0

Contents

1. Detailed Service Description

1.1 Overview

GlobalLogic provides end-to-end Security Quality Assurance and Testing services designed to identify, assess and mitigate risks within complex cloud and digital ecosystems. Our approach integrates security into the DNA of client products and processes, moving beyond "point-in-time" assessments to continuous assurance.

We combine automated tooling with expert manual analysis to cover the full spectrum of modern threats, from **OWASP Top 10 vulnerabilities** in web applications to supply chain risks in open-source dependencies. Our services support compliance with rigorous standards including the NCSC's Cyber Assessment Framework (CAF), ensuring operational resilience for public sector workloads.

1.2 Scope of the Service

Our security testing capabilities cover the entire software development lifecycle (SDLC):

- **Application Security**: SAST and DAST for web, mobile and API layers using industry-standard tools.
- **Infrastructure Hardening**: Vulnerability scanning and configuration review against CIS Benchmarks for hosts, networks and containers.
- **Penetration Testing**: Ethical hacking to exploit vulnerabilities in business logic, authentication and access controls.
- **DevSecOps**: Integration of security gates into CI/CD pipelines for automated code scanning and compliance checks.
- **Supply Chain Security**: Analysis of third-party libraries and open-source components to detect known vulnerabilities (CVEs) and license risks.

1.3 Delivery Approach

We utilise a risk-based methodology aligned with NIST 800-30 and industry best practice:

1. **Discovery & Threat Modelling**: We analyse system architecture to identify assets, entry points and potential threats (e.g. STRIDE model).
2. **Assessment Execution**: Parallel execution of automated scans (SAST/DAST) and manual penetration testing to identify false positives and complex logic flaws.
3. **Analysis & Reporting**: Findings are validated, scored by criticality (CVSS) and mapped to specific remediation actions.
4. **Remediation Support**: We collaborate with engineering teams to fix issues and perform re-testing to verify successful mitigation.

1.4 Tools, Methods & Standards

Our practice utilises a comprehensive toolset aligned to specific testing requirements:

- **SAST**: Checkmarx, SonarQube, HP Fortify SCA, FindSecBugs.
- **DAST & Pen Testing**: Burp Suite, OWASP ZAP, Metasploit, Kali Linux, Nessus, nMap.
- **Network Analysis**: Wireshark, AirCrack-ng.
- **Standards & Guidelines**: ISO 27001, Cyber Essentials Plus, CIS Benchmarks, **OWASP Top 10**.

1.5 Deliverables

- **Security Test Plan**: Defining scope, rules of engagement and testing methodology.
- **Vulnerability Report**: Detailed technical findings with CVSS scores, evidence and reproduction steps.
- **Executive Summary**: High-level risk profile and strategic recommendations for stakeholders.
- **Remediation Roadmap**: Prioritised backlog of fixes aligned to release schedules.
- **Compliance Statement**: Evidence of alignment to required standards (e.g. GDPR, PSN).

1.6 Dependencies & Constraints

- Client must provide authorised access to relevant environments, code repositories and documentation.

- Testing windows must be agreed in advance to minimise impact on live services.
- "White box" testing requires architectural diagrams and source code access.
- Third-party components/hosting may require explicit permission for penetration testing.

1.7 Customer Responsibilities

- Nominate a technical point of contact for the duration of testing.
- Approve the Rules of Engagement (RoE) prior to test commencement.
- Provide test data or non-production accounts to avoid data corruption risks.
- Review and accept findings within agreed timescales.

1.8 Quality Assurance & Governance

GlobalLogic employs a dedicated security practice lead to oversee all engagements. All reports undergo a peer review process to ensure accuracy and clarity. We utilise a Traceability Matrix to ensure all requirements and compliance guidelines are fully tested and evidenced.

1.9 Security, Data Protection & Compliance

We operate under strict ISO 27001 and Cyber Essentials Plus certified controls. All findings are treated as highly confidential. Data handling complies with UK GDPR; sensitive test data is encrypted in transit and at rest, and securely destroyed upon engagement completion. Staff hold relevant security clearances (BPSS/SC) as required.

---

2. Onboarding & Offboarding

2.1 Onboarding

Our onboarding process ensures rapid mobilisation:

1. **Kick-off Workshop**: Define scope, objectives and Rules of Engagement.
2. **Access Provisioning**: Setup of VPNs, user accounts and tool integration.
3. **Environment Validation**: Sanity check of test environments and connectivity.
4. **Team Mobilisation**: Assignment of security engineers and testers.

2.2 Offboarding

1. **Handover Workshop**: Walkthrough of findings and remediation advice.
2. **Data Clean-up**: Secure deletion of all client data and credentials from GlobalLogic systems.
3. **Access Revocation**: Return of all tokens, keys and accounts.
4. **Final Sign-off**: Client acceptance of final reports and deliverables.

3. Pricing & Commercials

This service is priced on a **Time & Materials** basis aligned to the GCloud Rate Card embedded in our G-Cloud listing. Rates vary by consultant grade (e.g. Junior Tester vs. Principal Security Architect).

4. Case Studies

4.1 Telecom Vendor - Security Hardening & Pen Testing

GlobalLogic delivered web penetration testing and system hardening for a Service Operations Center solution. We performed vulnerability management, network scanning and hardening against CIS benchmarks, achieving 90% compliance and ensuring the solution was ready for external production deployment.

5. About GlobalLogic & Why We're the Right Partner

5.1 About GlobalLogic

GlobalLogic, a Hitachi Group Company, is a leader in digital product engineering. We helped create some of the most innovative and widely used digital products and experiences. We integrate experience design, complex engineering and AI & data expertise to help public sector organisations and commercial enterprises accelerate their transition into digital-first businesses.

Unlike traditional systems integrators that focus on maintaining legacy IT, we focus on **building the new**. We combine a "chip-to-cloud" software engineering mindset with user-centric design to create digital products that citizens and employees want to use.

- **Global Scale, Local Delivery:** We employ over 32,000 professionals across 23 countries. In the UK & Ireland, we operate major engineering and design hubs in London, Manchester, Edinburgh, and Newry.
- **The Hitachi Advantage:** Acquired by Hitachi in 2021, we bring the agility of a Silicon Valley digital native backed by the financial stability, R&D depth and 110-year heritage of a global industrial giant.
- **Core Capabilities:** Our services span the full digital lifecycle, including Digital Advisory, Experience Design (via our Method design arm), Software Engineering, Data & AI, and Cloud Platform development.

5.2 Why GlobalLogic

We bridge the gap between strategic intent and technical execution. For public sector buyers, we offer a distinct alternative to incumbent providers by focusing on **delivery velocity** and **engineering rigour**.

- **We Build, We Don't Just Advise:** Our roots are in product engineering. We apply the same rigorous standards used to build life-critical medical devices and global banking platforms to public sector challenges. We deliver working software, not just slide decks delivering >2000 product releases per annum.
- **Velocity AI – Accelerating Impact:** We do not just build AI; we engineer ecosystems where intelligence is orchestrated across the business. Using our Velocity AI strategy, we typically

achieve a 30% increase in productivity and a 25% reduction in time-to-market for new digital services.

- **User-Centric, Security-First:** We align with GDS (Government Digital Service) standards by default, ensuring services are accessible and intuitive. Crucially, we embed security into the engineering lifecycle (Secure-by-Design), aligning with NCSC principles to manage data and risk effectively.

- **Proven in Regulated Environments:** We have two decades of experience delivering in highly regulated sectors, including Life Sciences, Healthcare, and Financial Services. We understand how to navigate complex compliance landscapes without sacrificing the pace of innovation and hold (amongst others) **ISO 13485 certification** and follow **IEC 62304 compliant** software development lifecycles.

5.3 Social Value & Ethical Impact

We believe that social innovation is as critical as technical innovation. GlobalLogic, as part of the Hitachi Group, operates with a deep commitment to creating positive impact for people and the planet. Our approach is grounded in measurable outcomes and global ethical standards.

- **World-Class Ethical Leadership:** In 2025, Hitachi was named one of the **World's Most Ethical Companies** by Ethisphere. This recognition reflects our commitment to integrity, compliance and high standards of governance in every public sector engagement.

- **Commitment to Diversity and Inclusion:** We are a signatory of the **CEO Action for Diversity and Inclusion**. We achieved the Hitachi Group 2030 goal of having **30% women in our workforce** in 2023, seven years ahead of schedule.

- **Sustainable Operations:** GlobalLogic holds an **EcoVadis Silver Rating**, placing us in the **top 15%** of companies assessed for sustainability in our sector. We report our own Scope I, II and III emissions and are fully aligned with Hitachi's target to achieve carbon neutrality at all business sites by 2030.

- **Proven Supply Chain Integrity:** Our **NQC Supplier Assurance** score exceeds the industry average by **25%**. This ensures that our delivery models are as responsible as they are resilient.

- **Talent Development and Wellbeing:** GlobalLogic is recognized as a global leader in talent development, receiving the **ATD Best Award in 2025**. This ensures our public sector teams are continuously upskilled in the latest technologies, including responsible AI and secure engineering practices.

6. Contact Details

Email: public.sector@globallogic.com
Website: www.globallogic.com/uki