GlobalLogic®
A Hitachi Group Company

Cloud Platform Security Remediation (AWS & Azure)

SERVICE DEFINITION DOCUMENT - VERSION 1.0

Contents

1. Detailed Service Description

1.1 Overview

The **Cloud Platform Security Remediation (AWS & Azure)** service provides a specialised, hands-on engineering capability designed to eliminate historic backlogs of Critical and High-severity cloud security vulnerabilities. Unlike advisory-only engagements, GlobalLogic provides the technical execution power to patch, configure, and secure cloud assets directly.

We target the four highest-risk asset categories: Virtual Machines, Container Images, Running Containers, and Serverless Functions. By combining automated discovery (via CSPM tools like Wiz) with standardised remediation playbooks, we rapidly transition your cloud estate from a reactive state of "technical debt" to a proactive posture of **30-day compliance** (where no critical vulnerability remains unresolved for more than 30 days).

1.2 Scope of the Service

This service focuses on the technical remediation of infrastructure and platform vulnerabilities within AWS and Azure environments.

In-Scope Asset Categories:

- **Virtual Machines (VMs):** OS-level patching, package updates, and configuration hardening.
- **Container Images:** Identification of vulnerable base images/layers and updating build manifests (e.g. Dockerfiles).
- **Running Containers:** Coordination of redeployment cycles to replace vulnerable runtime instances with secured images.
- **Serverless Functions:** Updating vulnerable libraries/dependencies and rectifying insecure configurations.

Service Boundaries:

- **Remediation Focus:** Critical and High-severity vulnerabilities only.
- **Exclusions:** Complex application code re-architecture or re-writing (defined as fixes requiring >15 minutes of coding effort) to ensure operational stability.

1.3 Delivery Approach

We utilise a structured, iterative remediation lifecycle designed to maximise velocity while minimising risk to live services.

- **Discovery & Triage:** Ingestion of vulnerability data from your CSPM (e.g. Wiz); prioritisation based on severity, age, and exposure; creation of the **Prioritised Roadmap**.
- **Design (Playbooks):** Development of **Standardised Remediation Playbooks** for each asset type. These define the "Standard Operating Procedure" for fixing specific vulnerability classes, ensuring consistency.
- **Build (Remediation):** Hands-on execution of fixes. Engineers access the environment to apply patches, update manifests, and modify configurations in lower environments first.
- **Test & Validation:** Verification of fixes using the CSPM tool to confirm the vulnerability status has moved to "Resolved".
- **Transition:** Promotion of fixes to production (via Change Management) and handover of updated documentation for ongoing maintenance.

1.4 Tools, Methods & Standards

We align with NCSC Cloud Security Principles and industry-standard DevOps practices.

- **CSPM Tooling:** We integrate with your existing tooling (e.g. Wiz, Prisma Cloud, Microsoft Defender) as the "source of truth".
- **Infrastructure as Code (IaC):** Terraform, AWS CloudFormation, Azure ARM for persistent configuration updates.
- **CI/CD:** Jenkins, Azure DevOps, or AWS CodePipeline for automated build and deployment of secured assets.
- **Containerisation:** Docker, Kubernetes (EKS/AKS).
- **Standards:**
    - **NCSC Cloud Security Principles**
    - **Secure-by-Design** methodology
    - **CIS Benchmarks** for configuration hardening

1.5 Deliverables

- **Prioritised Remediation Roadmap:** A strategic plan detailing the sequencing of fixes to maximise risk reduction.
- **Standardised Remediation Playbooks:** Documented, repeatable procedures for resolving specific vulnerability types across VMs, Containers, and Serverless.
- **Remediation Execution:** The physical application of patches and configuration updates to agreed assets.
- **Validation Reports:** CSPM-generated evidence confirming the reduction in vulnerability counts and "Resolved" status.
- **Burndown Reporting:** Weekly metrics tracking the reduction of the vulnerability backlog against the 30-day compliance target.

1.6 Dependencies & Constraints

- **Access:** The Client must provide GlobalLogic engineers with appropriate RBAC/IAM permissions (e.g. Contributor/Power User) to perform remediation actions in AWS/Azure.
- **CSPM Access:** Read-only access to the Client's CSPM tool is required for triage and validation.
- **Change Management:** The Client is responsible for the timely review and approval of Change Requests (CRs) to allow deployment of fixes to production environments. Delays in CR approval may impact 30-day targets.
- **Application Knowledge:** Access to Client application SMEs may be required to validate that applied patches do not impact application functionality.

1.7 Customer Responsibilities

- Nominate a Product Owner to prioritise the backlog and approve Playbooks.
- Facilitate access to cloud environments and security tooling.
- Provide maintenance windows for remediation activities requiring service restarts.

- Manage internal communication with application teams regarding deployment schedules.

1.8 Quality Assurance & Governance

- **Validation Source of Truth:** All fixes are validated against the CSPM tool. A fix is only considered "Complete" when the CSPM reports the vulnerability as resolved.
- **Playbook Validation:** All remediation playbooks undergo peer review and testing in non-production environments before general application.
- **Weekly Governance:** Regular status reviews to track the "Vulnerability Burndown" rate, discuss blockers, and manage risk.
- **SLA Monitoring:** Continuous tracking of vulnerability age to ensure adherence to the 30-day compliance mandate.

1.9 Security, Data Protection & Compliance

- **Security Clearance:** All staff are screened to BPSS as a minimum. SC-cleared staff are available upon request.
- **Data Handling:** No live customer data is extracted or processed on GlobalLogic devices. All remediation occurs within the Client's secure cloud tenant.
- **Standards:** Our delivery centres are ISO 27001 and ISO 9001 certified. We hold Cyber Essentials Plus (CE+) certification.
- **Least Privilege:** We operate under a Principle of Least Privilege (PoLP), requesting only the permissions necessary to execute specific remediation tasks.

---

2. Onboarding & Offboarding

2.1 Onboarding

- **Kick-off Workshop:** Confirm scope, targets, and "definition of done" for the backlog.
- **Access Provisioning:** Setup of IAM/RBAC accounts and VPNs for GlobalLogic engineers.
- **Tooling Integration:** Connection to Client CSPM and backlog management tools
- **Initial Triage:** First scan and prioritisation of the vulnerability backlog.

2.2 Offboarding

- **Knowledge Transfer:** Handover of all Remediation Playbooks and documentation to internal teams.
- **Final State Report:** A concluding report detailing the final security posture, total vulnerabilities remediated, and remaining residual risk.
- **Access Revocation:** Removal of GlobalLogic accounts and permissions from Client environments.
- **Data Deletion:** Secure deletion of any local project data in line with ISO 27001 standards.

3. Pricing & Commercials

- **Pricing Model:** Time & Materials or Fixed price for agreed scope based on the GCloud rate card.
- **Rate Card:** Please refer to the separate **Pricing Document** and **GCloud Rate Card** uploaded to the Digital Marketplace.

---

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

4.1 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.

4.2 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.

4.3 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.

5. Contact Details

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