GlobalLogic®
A Hitachi Group Company

# Cloud Security Design and Foundation (AWS): Guardrails & Governance

*SERVICE DEFINITION DOCUMENT - VERSION 1.0*

## Contents

# 1. Detailed Service Description

## 1.1 Overview

GlobalLogic provides a specialised service to design and implement secure-by-design AWS foundations, focusing on governance, compliance, and automated security guardrails. We help public sector organisations mitigate "account sprawl" and inconsistent security postures by deploying a centralised governance model using AWS Control Tower and AWS Security Hub. This service aligns your cloud environment with NCSC Cloud Security Principles and industry standards (ISO27001, Cyber Essentials Plus) from the outset. It establishes a "single source of truth" for security visibility, enforcing preventive and detective controls that empower development teams to innovate safely within defined boundaries.

## 1.2 Scope of the Service

This service delivers a comprehensive security and governance framework for your AWS estate, including:

- **Security Baseline Design**: Definition of a robust security baseline tailored to your specific compliance requirements (e.g., OFFICIAL, NHS DSPT).
- **Automated Guardrails:** Deployment of preventive guardrails (Service Control Policies) and detective guardrails (AWS Config Rules) via AWS Control Tower to prevent non-compliant resource creation.
- **Identity & Access Management (IAM):** Implementation of AWS IAM Identity Center (SSO) for centralised user access, enforcing Multi-Factor Authentication (MFA) and least-privilege principles.
- **Centralised Security Operations:** Configuration of AWS Security Hub, Amazon GuardDuty, and Amazon Inspector for centralised threat detection and vulnerability management.
- **Compliance Reporting**: Deployment of automated compliance conformance packs (e.g., CIS Benchmarks) to provide real-time visibility into your compliance posture.
- **Secure Networking:** Design of secure VPC patterns, Transit Gateway attachment rules, and firewall policies to isolate sensitive workloads.
- **Logging & Auditing:** Establishment of an immutable, centralised log archive (CloudTrail, VPC Flow Logs) to ensure forensic readiness and auditability.

## 1.3 Delivery Approach

We deliver this service using a phased approach to ensure security controls are implemented without disrupting business velocity:

1. **Security Discovery**: We review your existing security posture and compliance requirements to define the target guardrail strategy .
2. **Design & Policy Definition**: We produce a Security High-Level Design (HLD) detailing the Organisation structure (OU), SCPs, and IAM roles.
3. **Build & Configure:** We deploy the Landing Zone foundation, enable Control Tower, and configure the security toolset (Security Hub, GuardDuty).
4. **Guardrail Deployment:** We roll out the agreed preventive and detective controls, testing them to ensure they effectively block or flag non-compliant actions.
5. **Transition**: We handover operational runbooks and conduct knowledge transfer sessions with your SecOps team.

---

## 1.4 Tools, Methods & Standards

We leverage cloud-native security services and best-practice frameworks:

- **Core Services:** AWS Control Tower, AWS Organizations, AWS IAM Identity Center.
- **Security Services:** AWS Security Hub, Amazon GuardDuty, AWS Config, Amazon Macie.
- **Frameworks**: NCSC Cloud Security Principles, CIS AWS Foundations Benchmark, AWS Well-Architected Framework (Security Pillar).
- **Automation**: Terraform or CloudFormation for Infrastructure as Code (IaC) deployment of security controls.

---

## 1.5 Deliverables

- **Security Architecture Definition:** Comprehensive design document covering IAM, Network, and Compliance.
- **Governance Framework:** Documented hierarchy of Service Control Policies (SCPs) and Config Rules.

- **Deployed Security Foundation:** Operational AWS environment with live security services and guardrails.
- **Compliance Dashboard:** Configured AWS Security Hub providing a unified view of security alerts and compliance status.
- **Operational Runbooks**: Guides for managing user access, responding to GuardDuty alerts, and handling non-compliant resources.

---

## 1.6 Dependencies & Constraints

- **Root Access:** We require root email addresses and administrative access to the management account to configure AWS Organizations.
- **Security Stakeholders:** Availability of your CISO or Information Security representatives to approve policy definitions.
- **Identity Provider:** Access to your existing Identity Provider (e.g., Azure AD, Okta) for SSO integration.
- **Legacy Accounts:** If retrofitting governance to existing accounts, "brownfield" constraints may apply requiring a specific migration planning phase.

---

## 1.7 Customer Responsibilities

- Define specific internal compliance policies that must be enforced (e.g., specific regions, allowed instance types).
- Provide timely approval for security policies and guardrail definitions.
- Ensure availability of internal network teams if VPN/Direct Connect integration is required.
- Participate in security workshops and acceptance testing.

---

## 1.8 Quality Assurance & Governance

- **Security Design Review:** All designs are reviewed by a Lead Security Architect against NCSC principles.

- **Configuration Validation:** Automated testing of guardrails to ensure they correctly allow/deny specific API actions.
- **Compliance Scanning:** Post-deployment scan using Prowler or AWS Security Hub to verify the baseline security posture.
- **Governance Meetings:** Regular checkpoints to track progress, risks, and alignment with business objectives.

---

## 1.9 Security, Data Protection & Compliance

- **Data Residency**: All data and resources are pinned to UK/EU regions to meet sovereignty requirements.
- **Encryption**: Enforced encryption at rest (KMS) and in transit (TLS 1.2+) for all relevant services.
- **Least Privilege**: User access is granted strictly on a need-to-know basis using temporary credentials via SSO.
- **Audit Trail:** Comprehensive logging of all actions enables detailed forensic analysis and supports GDPR compliance.

---

# 2. Onboarding & Offboarding

## 2.1 Onboarding

1. **Security Workshop**: We commence with a discovery session to map your compliance landscape and identify specific risks.
2. **Prerequisites Check**: Verification of access rights, AWS account limits, and identity provider readiness.
3. Baseline Definition: Agreement on the initial set of guardrails (e.g., "Deny public S3 buckets").

## 2.2 Offboarding

1. **Handover**: Full transfer of all Infrastructure as Code (IaC) repositories and design documentation.
2. **Knowledge Transfer:** Sessions with your security team to explain the guardrail logic and alert response procedures.
3. **Account Transfer:** Seamless handover of the AWS management account credentials and root user tokens.

---

# 3. Pricing & Commercials

**Pricing Model**: Time & Materials (T&M) based on the GCloud-15 Rate Card or Fixed price based on agreed scope and the GCloud 15 rate card.

# 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