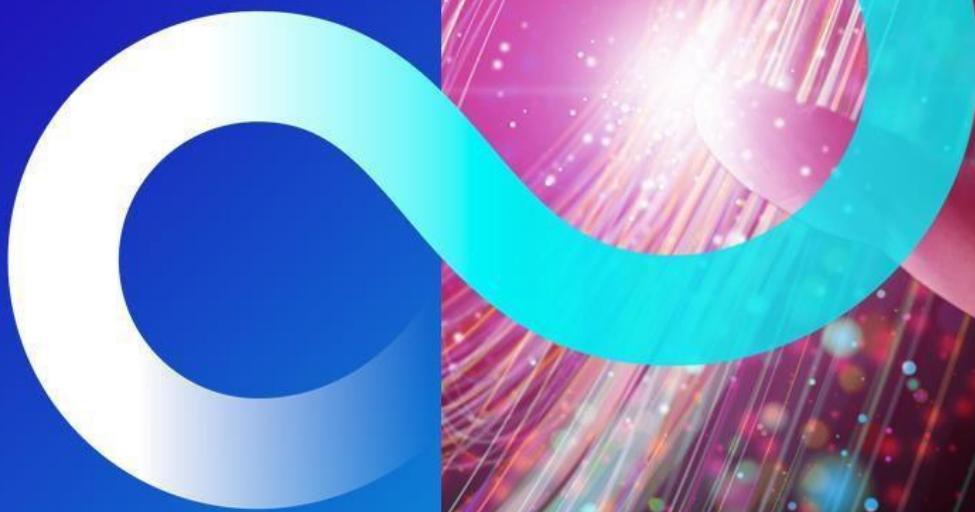


Service Definition

UK Cloud Governance Service (Lite)

FUJITSU



G-Cloud 15

© Fujitsu 2026

Contents

UK Cloud Governance (Lite) Overview 3

Service Delivery Approach 4

Service Deliverables 5

Commercial 6

UK Cloud Governance (Lite) Overview

This is a UK-delivered cloud governance service designed to establish and operate a practical governance operating model across cloud environments. It focuses on two outcomes: (1) a controlled, auditable cloud posture (policy, compliance and operational guardrails), and (2) an operational FinOps discipline to improve cost transparency and reduce waste. The service provides governance control and reporting; it does not replace platform operations (AWS/Azure Managed Service) or security operations (SOC/SIEM).

Who is this service for: UK organisations using public cloud (AWS and/or Azure) that need repeatable governance, evidence and cost control without turning governance into a never-ending consultancy engagement.

What this service is: A governance layer that sets baselines, monitors compliance and cost signals, manages exceptions, and runs a governance cadence (reports, reviews and decision forums).

What this service is not: A migration programme, an architecture redesign service, a Service Desk, or a SOC. Application defect fixing and day-to-day platform operations sit outside this service unless separately contracted.

In scope: Governance enablement and baseline definition; policy and standards alignment; posture monitoring and compliance reporting; FinOps reporting and cost guardrails; governance forums and decision support; exception handling; evidence pack production.

Out of scope: Hands-on platform build/migration work, large-scale remediation programmes, procurement/licensing management, SOC/SIEM operations, forensic investigations, and management of non-cloud estates unless separately contracted.

Service modules: The service is delivered through the following governance modules (activated as required).

Module	What it covers
Posture baseline and control objectives	Minimum control set aligned to customer risk appetite; standards mapping and control ownership.
Policy and guardrails operations	Policy definition/maintenance, compliance reporting, drift tracking and remediation recommendations.
Identity and access governance (governance view)	Role model governance, privileged access principles and access review cadence (execution via platform teams).
Data and logging governance	Telemetry retention principles, logging expectations and evidence requirements; routing decisions owned by the customer.
FinOps (operational) governance	Cost allocation approach, tagging standards, budget/alert guardrails, trend reporting and optimisation backlog.
Exception and risk management	Exception workflow, risk register entries, decision logs and expiry/review controls.
Governance reporting and forums	Monthly governance pack, decision forums, QBR inputs (if required).

Service Delivery Approach

Delivery model: Delivered remotely by UK-based governance specialists. The service operates primarily in core hours (Mon–Fri 08:00–18:00 UK time). Where 24x7 incident handling is required, this is provided by the relevant managed service (AWS/Azure) or the customer's Service Desk; governance provides escalation and decision support via agreed on-call arrangements if contracted.

Engagement phases:

- 1) Governance assessment and enablement: confirm scope, stakeholders, decision forums, and baseline control objectives.
- 2) Baseline definition: agree minimum control set, standards, and governance artefacts (policies, templates, reporting pack).
- 3) Instrumentation and evidence: configure/validate reporting sources and evidence capture mechanisms (native tooling baseline).
- 4) Operate: run governance cadence (monthly pack, forums), manage exceptions, and maintain the optimisation backlog.
- 5) Improve: track actions and trends; revise controls as the environment or risk posture changes.

Native tooling baseline: The service uses hyperscaler-native reporting and governance features as the default evidence source (e.g., Azure Policy/Advisor/Cost Management and AWS Config/Security Hub/Budgets/Cost Explorer). Where customer enterprise tooling is used, the customer provides licensing and access; integration work may be chargeable.

Decision governance: This service provides recommendations and decision support. Risk acceptance, exception approvals and policy targets remain the customer's responsibility. If a customer requests the supplier to execute changes, those changes are delivered through the appropriate managed service or separately scoped project work.

Reporting cadence (baseline): Monthly governance pack and service review as standard. QBR inputs and executive dashboards are available by agreement.

Service Deliverables

The following are delivered at the conclusion of the Assessment:

- Governance scope and operating model: stakeholders, RACI, forums, decision rights and cadence.
- Minimum Control Set (baseline): control objectives and policy intents aligned to customer risk appetite.
- FinOps baseline: tagging/allocation approach, budget/alert guardrails and initial cost reporting view.
- Exception workflow: exception request template, approval route, review/expiry approach and evidence expectations.
- Evidence plan: what evidence is produced, where it is sourced from and how often it is generated.
- Initial governance reporting pack: baseline posture view, cost signals, risks, exceptions and action backlog.

Ongoing run-state deliverables include:

- Monthly governance pack: posture/compliance trends, exceptions, risks and actions.
- FinOps reporting: allocation visibility, budgets/alerts review, optimisation backlog tracking.
- Policy and standards maintenance: baseline updates, drift monitoring and remediation recommendations.
- Exception and risk management: decision log, exception reviews/expiry handling and risk register updates.
- Governance forums: monthly service governance meeting outputs and QBR inputs where contracted.

Commercial

Commercial model (summary): The service is typically priced as a one-off Governance Assessment/Enablement charge plus a recurring governance operations charge. Recurring pricing is driven by the number of cloud environments in scope (accounts/subscriptions/management groups), reporting depth, and the required governance cadence. Remediation execution and engineering work are out of scope unless separately contracted.

Typical charging units (indicative):

Element	Charging unit	Notes
Assessment and enablement	Per engagement / per environment	One-off baseline set-up, scope, artefacts and reporting pack.
Governance operations	Per environment (monthly)	Monthly pack, forums, exception handling and backlog management.
FinOps uplift (optional)	Per environment (monthly) or T&M	Deeper optimisation cycles, chargeback/showback support and commitments review.
Policy/controls uplift (optional)	T&M or fixed scope	Non-standard standards mapping, control framework alignment, bespoke reporting.

Ordering and Invoicing Process

- We will commence delivery of the service on receipt of a purchase order
- Fujitsu shall invoice for the Service plus any applicable taxes after delivery of all our products defined in the agreed Terms of reference. Any additional expenses shall be invoiced in the month after they have been incurred
- The customer will pay the invoiced amount in full within thirty (30) days of the date of each invoice (the “Due Date”)
- If the customer has not paid Fujitsu an invoice by its Due Date, Fujitsu may charge interest on a day-to-day basis from the due date at the rate of 4% per annum over the Barclays Bank Base Rate until the payment is made in full
- The customer shall not be entitled to offset any sums owed by Fujitsu under any contract or dispute between the customer and Fujitsu against any sums that the customer owes to Fujitsu
- When remitting payment, the customer will include the applicable Fujitsu invoice that the payment applies to

Customer Termination

The Customer may terminate this Agreement (or any part thereof), at any time, for convenience by giving not less than thirty (30) days written notice to Fujitsu.

Supplier Termination

Fujitsu may terminate this Agreement (or any part thereof), at any time, for convenience by giving not less than thirty (30) days written notice to the Customer.

Consumer Responsibilities

Successful delivery of the Service is subject to the following dependencies upon the Customer:

- Provide a Service Desk or ticketing function as a single point of contact and to control governance request/decision flow (24-hour coverage required only where the customer requires 24x7 governance escalation).
- Provide cloud billing access and cost allocation inputs (e.g., billing export/enrolment data, cost centre mappings, subscription/account ownership).
- Provide (or separately contract) reporting and alerting tooling where Fujitsu-defined native governance reporting is not used.
- Ensure High-Level Design (HLD) and Low-Level Design (LLD) documentation for the environments in scope are available, plus any customer-specific standards and policies.
- Provide required cloud access (least privilege) to the governance scope (management groups/organisations, policy assignment scope, reporting workspaces).
- Nominate governance stakeholders with decision rights (risk acceptance, exception approvals, policy targets) and ensure attendance at governance forums.
- Maintain vendor support contracts for in-scope components where applicable; End of Support items are treated with

reduced coverage and may incur uplifts where remediation execution is requested.

Service Constraints

- Only cloud environments formally onboarded into governance scope are governed and reported.
- Only controls/policies formally agreed as part of the baseline are operated under this service; changes require formal approval via the agreed governance process.
- This service provides governance, reporting and recommendations; execution of engineering remediation is out of scope unless separately contracted.

Service Exclusions

- **Engineering execution / remediation:** we provide governance, reporting, recommendations and decision support; we do **not** implement platform changes, fixes, patching, reconfiguration or build work unless separately contracted (or delivered via an AWS/Azure Managed Service tower).
- **Migrations and transformation programmes:** landing zone builds, re-architecture, large remediation programmes, data centre exits, platform re-platforming or tooling rollouts are out of scope.
- **Service Desk / ITSM tool provision:** we don't provide the ticketing platform or a user-facing Service Desk; we can operate through your existing ticket flow and governance forums.
- **Security operations:** no SOC/SIEM operations, threat hunting, incident response, malware analysis, forensics, eDiscovery or legal hold.
- **Procurement and licensing management:** we don't purchase, resell or manage cloud licences/contracts; we can provide governance inputs (e.g., consumption trends and recommendations).
- **Non-cloud scope:** on-prem infrastructure, networks, endpoints, EUC, and non-cloud platforms are out of scope unless explicitly included as a separate service.
- **Application delivery:** no application development, code remediation, release engineering or CI/CD ownership; any app reliability work is out of scope unless separately contracted (e.g., SRE).
- **Customer decision ownership:** we do not take accountability for risk acceptance, exception approvals or policy targets — those remain customer decisions (we provide the evidence and recommendation).
- **Anything not formally onboarded to governance:** if an account/subscription/management group isn't explicitly included in the governance scope, it isn't governed or reported on.
- **24x7 governance response:** the service is not a 24x7 operational response function; 24x7 monitoring/triage sits with your Service Desk and/or the managed service.

About Fujitsu

As one of the world's leading IT companies, Fujitsu is at the forefront of pioneering technology in the UK since we made our initial investment over 40 years ago. As a key strategic partner we deliver essential services, from our secure hybrid IT which underpins critical national infrastructure to our investment in emerging technologies to boost national capability. Drawing on our Japanese technology expertise we provide bespoke digital transformation solutions. This unrivalled expertise has allowed us to specialise in emerging focus areas; Hybrid IT, AI & RPA, Data analytics, Agile application development/transformation and Security. Together, we offer a full package of solutions to support the UK as a long-term industry supplier.

We believe in realising the significant alignment between the UK and Japan in emerging technologies and in creating a UK-Japan 'Innovation Bridge' to support the UK's science and technology superpower objectives. We are committed to investment in UK skills and research and development, driving customer outcomes and promoting social value. We employ 124,000 people around the globe, including around 8,000 people across the UK, promoting diversity and inclusion as a DWP Disability Confident Leader. We are recognised as a Times Top 50 employer for Women since 2017, a Stonewall Top 100 Employer for 2023 and were awarded an EcoVadis Silver Rating, the world's largest provider for sustainability ratings.

Contact: government.frameworks@fujitsu.com

FUJITSU-PUBLIC | Uncontrolled if printed.

© Fujitsu 2026 | All rights reserved. Fujitsu and Fujitsu logo are trademarks of Fujitsu Limited registered in many jurisdictions worldwide. Other product, service and company names mentioned herein may be trademarks of Fujitsu or other companies. This document is current as of the initial date of publication and subject to be changed by Fujitsu without notice. This material is provided for information purposes only and Fujitsu assumes no liability related to its use. Subject to contract. Fujitsu endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same. No part of this document may be reproduced, stored or transmitted in any form without prior written permission of Fujitsu Services Ltd. Fujitsu Services Ltd endeavours to ensure that the information in this document is correct and fairly stated, but does not accept liability for any errors or omissions.