

Service Definition: AI Managed Governance Service (MGS)

Contents

- Executive Summary 2
- UK Government Focus and Strategic Alignment 2
 - Alignment with UK Governance Frameworks: 2
- AI Technologies Covered 2
- Target Operating Model: The Integrated AI Council..... 3
 - Sample Terms of Reference (ToR)..... 3
 - Membership Personas:..... 4
 - AI / Agent Onboarding Workflow 4
- Service Catalogue: Core Managed Service vs. Service Requests 5
- Multi-Year Transition Roadmap 5
- AI Asset Inventory Template 5
- Service Backlog and Governance Delivery 6
- Operational Resilience and Exit Strategy 6
- Support and Pricing Structure 6
- Annual Service Fee (ASF)..... 7

Executive Summary

The Infotechtion AI Managed Governance Service (MGS) provides UK Public Sector organisations with a multi-year, proactive framework for managing Artificial Intelligence and autonomous agents. This service embeds Gartner’s TRiSM (Trust, Risk, and Security Management) and EU AI Act compliance into the departmental fabric, ensuring AI scaling is safe, ethical, and transparent. By moving beyond project-based consulting, we provide a permanent "governance-as-a-service" model that evolves alongside your technology landscape.

UK Government Focus and Strategic Alignment

This service is purpose-built to navigate the specific regulatory landscape of the UK Public Sector. We ensure that every AI implementation adheres to the core guardrails and principles established by the Central Digital and Data Office (CDDO) and the Department for Science, Innovation and Technology (DSIT).

Alignment with UK Governance Frameworks:

- **The AI Reform White Paper:** We operationalise the five core principles: Safety, Security and Resilience; Appropriate Transparency and Explainability; Fairness; Accountability and Governance; and Contestability and Redress.
- **CDDO Algorithmic Transparency Recording Standard (ATRS):** We automate the collection and formatting of data required for mandatory transparency reporting, ensuring public-facing records are accurate and up-to-date.
- **GDS Service Standard:** We ensure AI-driven services meet Point 10 (Define the scope of the service) and Point 13 (Make the service secure) within the context of automated decision-making.
- **NCSC Guidelines for Secure AI:** We implement technical security controls required to protect government models from prompt injection, data poisoning, and model inversion.

AI Technologies Covered

The MGS provides specialized governance controls for a wide spectrum of AI technologies currently being deployed across the UK Government landscape:

Technology Category	Scope of Governance	Common Use Cases
---------------------	---------------------	------------------

Generative AI & LLMs	Prompt guardrails, data leakage prevention, and hallucination monitoring.	Policy drafting, briefing summaries, citizen chatbots.
Autonomous Agents	Authority-limit enforcement, multi-agent orchestration, and "kill-switch" protocols.	Automated workflow execution, digital personal assistants.
Predictive Analytics	Bias detection in training sets, drift monitoring, and statistical validity audits.	Fraud detection, resource allocation, risk modeling.
Computer Vision	Privacy-masking validation, accuracy auditing, and ethical usage reviews.	Secure facility access, document digitization.
NLP & RPA	Entity recognition accuracy and exception handling governance.	FOI request sorting, public consultation analysis.

Target Operating Model: The Integrated AI Council

To ensure AI onboarding is process-driven, Infotechtion establishes and facilitates an **AI Governance Council** integrated into existing corporate governance to prevent silos.

- **The AI Council:** Central "Clearing House" for all AI/Agent initiatives.
- **Architecture Integration:** Ensures models align with departmental data standards (CDDO) and interoperability requirements.
- **Security Integration (SIRO/CISO):** Validates AI-specific security controls against adversarial attacks.
- **Privacy Integration (DPO):** Ensures compliance with UK GDPR and EU AI Act fundamental rights mandates.

Sample Terms of Reference (ToR)

- **Purpose:** To provide ethical, legal, and technical oversight for AI and agents.
- **Mandate:** The final arbiter for all AI "Go/No-Go" decisions within the department.
- **Quorum:** Decisions require the Chair, DPO, and SIRO to be present to ensure cross-functional consensus.

- **Escalation:** Matters involving "Unacceptable Risk" as defined by the EU AI Act are escalated to the Departmental Executive Board and SRO.

Membership Personas:

Persona	Role in the Council	Responsibility
Chief AI Officer (CAIO)	Council Chair	Strategic Lead; aligns AI usage with the departmental mission.
SIRO / CISO	Security Lead	Validates security controls against adversarial attacks and data leakage.
Data Protection Officer	Compliance Lead	Validates DPIAs and EU AI Act conformity.
Head of Architecture	Technical Lead	Confirms technical interoperability and data standard compliance.
Infotechtion TAM	Service Manager	Manages the service backlog and provides TRiSM audit data.

AI / Agent Onboarding Workflow

The service delivers a structured "Gate-Based" onboarding process to ensure every AI agent or application integrated into the technology landscape is vetted and governed.

1. **Discovery & Intent:** Proposal submission via the Service Catalogue.
2. **Classification (Agent Card):** Profiling autonomy, authority, and data access.
3. **Tiered Risk Assessment:** Categorisation (e.g., High-Risk per EU AI Act).
4. **TRiSM & Security Validation:** Technical testing for bias, explainability, and robustness.
5. **Council Adjudication:** Formal review by the integrated AI Council.
6. **Production Onboarding:** Registration in the Managed AI Risk Register.
7. **Continuous Audit:** Ongoing monitoring for drift and compliance.

Service Catalogue: Core Managed Service vs. Service Requests

Service Area	Included in Core Managed Service (MGS)	Available via Service Request (Ad-hoc)
Regulatory	Mandatory ATRS and EU AI Act monitoring.	Full Third-Party Conformity Assessments.
Risk & TRiSM	Continuous bias, drift, and accuracy monitoring.	Bespoke Adversarial Red-Teaming simulations.
Ethics	Quarterly Independent Ethics Board reviews.	Use-case specific Impact Assessments.
Security	Automated LLM Guardrail & prompt management.	Niche/Sovereign SLM technical integration.
Management	AI Risk Register & Backlog maintenance.	Custom FOI / Audit Response support.

Multi-Year Transition Roadmap

Phase	Focus Area	Key Milestones
Year 1: Foundation	Alignment & Setup	ISO 42001 alignment; Council establishment; "Shadow AI" discovery; baseline TRiSM controls.
Year 2: Scaling	Operationalisation	Automated bias monitoring in CI/CD; mandatory ATRS reporting automation; ALB expansion.
Year 3: Excellence	Optimisation	Predictive risk modeling; autonomous governance triggers; full GDS Service Standard maturity.

AI Asset Inventory Template

The MGS maintains a "Live" Inventory to satisfy Article 11 of the EU AI Act and the UK ATRS.

Column Header	Description
---------------	-------------

System ID & Name	Unique identifier and descriptive name of the AI application.
Owner & Vendor	Internal Product Owner and third-party provider details.
Risk Tier	Unacceptable, High, Limited, or Minimal risk with justification.
Model Type	e.g., Transformer, Random Forest, Agentic Orchestrator.
Data Lineage	Source datasets, PII classification, and residency (UK/EU).
Oversight Mode	Human-in-the-loop, Human-on-the-loop, or Human-in-command.

Service Backlog and Governance Delivery

To ensure roadmap evolution is managed and evidenced, all activities are tracked via a **Centralised Service Backlog**.

- **Prioritisation:** Ranked by Regulatory Deadlines (EU AI Act), Risk Scores, and Operational Impact.
- **Quarterly Value Realisation (QVR):** A formal 90-day review session to evidence completed controls and audit results.
- **The Evidence Vault:** A secure, audit-ready repository containing all ATRS records and conformity evidence for ICO or GDS inspection.

Operational Resilience and Exit Strategy

- **Operational Continuity:** In the event of a critical AI failure or "hallucination" event, the Sovereign support tier provides immediate incident response and model roll-back procedures.
- **Service Exit:** Upon termination, Infotechtion provides an "Exit Pack" containing all historical audit logs, the current AI Risk Register, and the Evidence Vault, ensuring no vendor lock-in and a seamless transition to internal teams.

Support and Pricing Structure

Support Tier	Scope	Cost Multiplier
Assurance	Business-hour technical support and core monitoring.	1.0x Base ASF

Strategic	Monthly TRiSM health checks and bi-annual policy refreshes.	1.4x Base ASF
Sovereign	24/7 security response and priority regulatory assessments.	1.8x Base ASF

Annual Service Fee (ASF)

Typically ranges from **£70,000 to £250,000** based on complexity, refer to pricing document for more details. Multi-year commitments (3-5 years) attract a **10-18% discount** for long-term budget stability.

Every engagement includes a dedicated **Technical Account Manager (TAM)** as your Governance Lead and access to **Cloud Support Engineers** for integration within Azure, AWS, or GCP.