Genesys DATA

Service Description
AI System Risk Snapshot

Scope

The AI System Risk Snapshot is a focused assessment that maps and scores an organisation's current use of AI and machine learning systems - whether internally built, third-party embedded, or vendor-managed. It identifies where AI is being used across the business, evaluates risks using structured criteria aligned to ISO/IEC 42001 (AI Management System) and NIST AI RMF (AI Risk Management Framework), and provides a baseline for regulatory, ethical, and operational readiness.

This service is ideal for organisations seeking to understand their AI footprint, prepare for future regulatory obligations (e.g. Privacy Act reforms, EU AI Act), or demonstrate responsible AI use to stakeholders.

Approach

The assessment is delivered over five structured phases, combining compliance alignment with practical discovery and prioritisation.

Initiation & Scoping

Sets the foundation for engagement by confirming focus, priorities, and stakeholders.

- **Define purpose -** compliance readiness, procurement due diligence, operational risk, governance uplift.
- **Confirm scope -** internal AI systems, embedded vendor tools, AI features in SaaS platforms.
- **Identify drivers -** regulatory (e.g. GDPR Article 22, Privacy Act & Automated Decision Making requirements), ethical, reputational, or strategic.
- Map key stakeholders: data stewards, IT, privacy, legal, procurement, business owners.
- **Establish definitions and thresholds** - for what qualifies as AI/automated decision-making.
- **Outputs -** Scoping matrix, stakeholder map, agreed definitions, success criteria.

Discovery & Inventory

This stage involves identifying, cataloguing, and assessing all AI systems in use.

- Conduct internal discovery to identify known and unknown AI systems (structured interviews, system review, business line surveys).
- Assess use cases, decision types, user impact, data sources, model ownership.

- Catalogue system characteristics - model type, training data, outputs, lifecycle stage.
- Capture documentation and governance artefacts (model cards, data sheets, contracts).

Risk & Maturity Assessment

AI systems are scored against risk criteria and maturity benchmarks.

- Evaluate systems against ISO 42001 and NIST AI RMF principles: transparency, fairness, security, accountability, reliability.
- Assess key risks - bias, drift, over-reliance, data quality, explainability, vendor lock-in.
- Score risk exposure using likelihood × impact × visibility.
- Map maturity across domains: governance, policy, controls, monitoring.

Validation & Prioritisation

This phase confirms findings and aligns priorities across teams.

- Review findings with key stakeholders to validate AI use cases and risk ratings.
- Adjust scoring based on context (e.g. population size, human override, public impact, internal risk settings).
- Prioritise systems requiring uplift or further assessment.
- Discuss potential remediation actions, owners, and timelines.

Reporting & Next Steps

Final results are presented and recommendations are prepared for implementation.

- Present findings to risk, data, or governance committees.
- Deliver a structured, board-ready summary of AI use, risks, and actions.
- Recommend governance structures, review cadences, and control uplift opportunities.
- Advise on integration with privacy, security, procurement, and risk workflows.
- Outputs: Final report, executive summary, AI governance uplift plan.

Value

The AI System Risk Snapshot helps organisations move from fragmented, reactive AI usage to a strategic, controlled, and accountable position. It provides foundational visibility and enables proactive risk mitigation.

- Highlights AI system visibility across embedded, internal, and shadow AI tools.
- Establishes a baseline of compliance readiness for future regulatory obligations.
- Identifies blind spots, high-risk use cases, and governance gaps early.
- Builds confidence for boards, customers, and partners around responsible AI use.
- Supports integration of AI oversight into existing privacy, security, and risk processes.

Benefits

The service delivers the following strategic and operational benefits.

- Gives immediate visibility into AI/ML system footprint across the business.
- Identifies regulatory risks and ethical red flags before issues arise.
- Supports procurement, investment, and innovation decisions.
- Reduces complexity and silos in AI governance practices.
- Enables prioritised action on AI governance, policy, and control gaps.

Outputs

Final deliverables will include the following items to drive ongoing action.

- AI System Risk Snapshot Report: Summary of AI systems, risks, and priority actions.
- AI System Inventory - Use case table, owners, model types, lifecycle status.
- Risk Scorecard - Per-system and aggregated risk exposure map.

Discovery & Risk Mapping

As part of delivering this service, a secure SaaS tenancy of the Data Governance / DSPM (Data Security Posture Management) platform may be provisioned, or tool connectors may be established through API integrations. This setup enables the registration, monitoring, and inspection of machine learning tools in use, as well as the configuration of governance workflows that support compliance reporting and risk scoring.

The DPSM is IRAP-assessed and SOC 2 Type II certified, ensuring alignment with recognised information-security and assurance frameworks. All traffic is encrypted in transit and governed under the client's enterprise security, privacy, and compliance controls.