Sovereign AI Shared Responsibility Model

Executive Summary

As Australian enterprise and government organisations deploy AI at scale, the boundary between platform responsibility and enterprise responsibility must be explicit. The **Songlines Control® Shared Responsibility Model** defines exactly what Cetus AI governs, and what the enterprise must enforce.

This model is designed to support procurement teams, CISOs, and risk assessors in evaluating AI governance boundaries, particularly for IRAP, QGEA, and APRA compliance.

The Four Layers of Responsibility

The boundary is delineated across four critical layers:

1. Platform Hosting (Cetus AI Responsibility)

Cetus AI is responsible for the secure, sovereign hosting of the Songlines Control® platform.

- **Data Sovereignty:** Ensuring all platform telemetry, logs, and configuration data remain within Australian borders.
- **Infrastructure Security:** Maintaining IRAP-aligned security controls for the platform infrastructure.
- **High Availability:** Delivering resilient architecture with guaranteed uptime SLAs.
- **Vulnerability Management:** Continuous patching and security testing of the Songlines platform.

2. Model Routing & Telemetry (Shared Responsibility)

Responsibility for how AI requests are routed and logged is shared.

- **Cetus AI:** Provides the infrastructure to route requests to approved models, capture telemetry, and generate immutable audit trails.
- **Enterprise:** Configures the routing rules, determines which models are approved for use, and reviews the audit trails for compliance.

3. Identity & Access (Enterprise Responsibility)

The enterprise retains full control over who can access AI resources.

- **Enterprise:** Manages user identities, configures role-based access control (RBAC) policies within Songlines, and handles authentication (e.g., via Entra ID/Active Directory).
- **Cetus AI:** Provides the RBAC enforcement engine that applies these enterprise-defined policies at runtime.

4. Enterprise Ecosystem & Data (Enterprise Responsibility)

The enterprise is responsible for the data fed into AI models and the downstream actions taken by AI agents.

- **Enterprise:** Defines what data is permissible for AI processing, configures PII redaction rules, and governs the actions of autonomous agents interacting with enterprise systems.
- **Cetus AI:** Provides the inline interception capabilities (like PII redaction) that the enterprise configures to protect its data.

Conclusion

By clearly delineating these responsibilities, Songlines Control® enables organisations to adopt AI rapidly while maintaining a defensible, board-reportable security and compliance posture.