[Title]

## AI Tool Evaluation Framework

### Shared decision lens for the AI Team and Chief Risk Officer to evaluate AI tools for use at Alceon

Alceon is pursuing an AI-native operating model by end of 2026. This one-pager establishes a shared, lightweight framework so the AI Team and CRO can quickly align on whether a tool is fit for purpose — without lengthy procurement cycles for low-risk use cases, while maintaining rigour for anything touching confidential or regulated data.

## 1. Data Classification Tiers

### The single question that determines the approval path: what data will enter the tool?

## 2. Evaluation Dimensions (Amber & Red Tools)

### For any tool that will handle internal or confidential data, assess against these dimensions.

|  |  |  |  |
| --- | --- | --- | --- |
| **Dimension** | **What We Assess** | **Amber** | **Red** |
| **Data Residency** | Where is data processed and stored? AU or compliant jurisdiction. | Preferred | Required |
| **Training Opt-Out** | Vendor confirms inputs are not used to train models. | Required | Required |
| **Security Certifications** | SOC 2 Type II, ISO 27001, or equivalent. | Preferred | Required |
| **Access Controls** | SSO / MFA integration and role-based access. | Preferred | Required |
| **Audit & Logging** | Activity logs available for compliance review. | Preferred | Required |
| **Data Processing Agreement** | Executed DPA with acceptable terms. | Preferred | Required |
| **Regulatory Alignment** | Consistent with Privacy Act, APRA guidance, AFSL obligations. | Required | Required |
| **Vendor Viability** | Established vendor with clear business model; not early beta. | Preferred | Required |
| **Exit / Off-boarding** | Data can be exported and deleted on termination. | Required | Required |

## 3. Non-Negotiables

**1. Human-in-the-Loop:** No AI output goes to a client, investor, counterparty, or regulator without qualified human review.

**2. No Confidential Data in Free Tools:** Consumer-grade or free-tier products must never touch Amber or Red data.

**3. Accountability Sits with the User:** The person using the tool owns the accuracy, compliance, and appropriateness of the output.

**4. Approved Tool List:** A living register of vetted tools maintained by the AI Team, reviewed quarterly with the CRO.

## 4. Decision Flow

Identify tier → Green: proceed | Amber/Red: assess against dimensions above → All “Required” items met? → Yes: approve and add to Approved Tool List | No: reject or escalate for risk acceptance.