ALIGN AI Assurance Field Manual

Explicit operational procedures for predictive, generative, third-party and agentic AI

Purpose and key distinction

AI governance must address uncertainty, changing models, feedback loops, emergent use, misuse and the ability of automated systems to take consequential actions. It cannot rely on data governance controls alone.

AI capability modules (original ALIGN language)

ID	AI capability	Primary ALIGN tier
AI-01	AI governance charter and risk appetite	Strategic
AI-02	AI inventory and classification	Foundational
AI-03	Business purpose and intended-use boundaries	Strategic
AI-04	Data use rights and provenance	Foundational
AI-05	Representative data and distribution checks	Foundational
AI-06	Model/solution ownership and suppliers	Foundational
AI-07	Impact and rights assessment	Tactical
AI-08	Evaluation design and acceptance thresholds	Tactical
AI-09	Robustness and adversarial challenges	Tactical
AI-10	Bias, subgroup and accessibility evaluation	Tactical
AI-11	Transparency and user notice	Tactical
AI-12	Human intervention and appeal	Tactical
AI-13	AI security / tool boundaries	Tactical
AI-14	Third-party terms and model change monitoring	Tactical

SAMPLE - SHARP ANALYTICS

© 2026 Sharp Analytics. All rights reserved. Do not copy or distribute without permission.

ALIGN Data & AI Governance Methodology℠ — created and owned by Sharp Analytics.

ALIGN Data & AI Governance Methodology™
Created and owned by Sharp Analytics.
© 2026 Sharp Analytics. All rights reserved. Do not copy or distribute without permission.

AI-15	Deployment gate and release record	Tactical
AI-16	Performance, drift and incident monitoring	Tactical
AI-17	Change, retraining and material-update controls	Tactical
AI-18	Retirement, archiving and termination	Tactical

Lifecycle gates: follow these procedures in order

Gate	Steps	Retained evidence	Stop / escalation
G0 Request and registration	Product owner logs intended users, decisions influenced, vendor/model, inputs, geography, affected people, tools/actions.	Inventory entry, accountable owner	Unapproved/shadow use => stop, isolate and triage
G1 Preliminary classification	Assess potential impact, legal exposure, sensitive information, degree of automation, external exposure and reversibility.	Risk screening; specialist routing	High-impact or prohibited application => escalated legal/risk review
G2 Data and design readiness	Check source lineage, data rights, quality, representativeness, permissions, retrieval boundaries and retention.	Data readiness record; architecture review	Unknown training rights or unauthorized data => block
G3 Evaluation and red-team	Design normal/edge-case tests, subgroup tests, leakage/prompt-injection tests, agent/tool-abuse tests and rollback tests.	Evaluation report with thresholds and failures	Unacceptable severity, safety defect or missing tests => block
G4 Controlled authorization	Product, security, legal/privacy and independent review as applicable; record residual risk and permitted population.	Signed gate record and time-bounded exceptions	Missing mandatory approver => no production
G5 Ongoing	Monitor quality,	Monthly system	Material change or

SAMPLE - SHARP ANALYTICS

© 2026 Sharp Analytics. All rights reserved. Do not copy or distribute without permission.

© 2026 Sharp Analytics. All rights reserved. Do not copy or distribute without permission.