

GOVERNING AI ACROSS AN ORGANIZATION

Scale the evidence with the AI.

Coordinate control evidence, independent challenge and improvement across a portfolio. Apply this wherever complexity or consequences justify it; advanced work does not require agents.

Portfolio / systems / affected people in scope

Accountable owner / shared dependencies

CONTROL AND EVIDENCE REGISTER

Risk / objective	Framework reference / control	Owner / covered systems	Evidence / scope / gap

A MAPPING IS NOT PROOF

Verify reference identifiers against the current framework. Distinguish a written policy, a deployed control and evidence that it works. Record dependencies and exceptions so shared failures can be traced to affected systems.

Evidence access restrictions / retention owner / review trigger

01 EVIDENCE

02 CHALLENGE

03 RISK

04 IMPROVE

05 RESOURCES

GOVERNING AI ACROSS AN ORGANIZATION

Invite meaningful challenge.

Define a review role with independence, information and authority to question decisions. Select internal audit, specialist review or another suitable arrangement. Reviewers need to understand the system's purpose, limitations and affected people.

Reviewer / independence and authority

Scope / evidence access / important limitations

Review area	Evidence / finding and rationale	Decision owner / action
Governance and accountability		
Evaluation and security testing		
Oversight and incident response		
Supplier and shared controls		

Unexamined assumptions / unavailable evidence / review limitations

CLOSE THE CHALLENGE WITH EVIDENCE

Check whether evaluations cover consequential failures, monitoring reaches real users and people can exercise promised oversight. Track findings through treatment and relevant retesting.

01 EVIDENCE

02 CHALLENGE

03 RISK

04 IMPROVE

05 RESOURCES

GOVERNING AI ACROSS AN ORGANIZATION

Accept remaining exposure explicitly.

After treatment, record the remaining exposure and who can accept it. Define acceptance boundaries, expiry and reconsideration triggers; retain the treatment rationale.

Residual risk / uncertainty / affected systems

Treatment evidence / alternatives considered

Accepting owner / authority / decision date

Conditions / expiry / review trigger

IF AGENTS CAN ACT - OPTIONAL ACTION BOUNDARY

Tool / action	Allowed resources / limits	Approval / stop / recovery	Test and audit evidence

ENFORCE ACTION RIGHTS OUTSIDE THE MODEL

Use minimum required rights. Test permission escalation, untrusted instructions, repeated actions, stopping and recovery. Confirm that approvals constrain the actual action. Agent adoption is a design choice.

Reconsider acceptance after relevant incidents, changed purpose, significant provider changes or evidence that assumptions no longer hold. Choose intervals suitable to your organization.

01 EVIDENCE

02 CHALLENGE

03 RISK

04 IMPROVE

05 RESOURCES

GOVERNING AI ACROSS AN ORGANIZATION

Make review change the system.

Combine portfolio visibility with measures suited to each task. Management review should decide on resources, priorities, unacceptable exposure and needed improvements.

Management signal	Source / limitations / owner	Review rule / decision
Failures and near misses		
Evaluation gaps / overdue reviews		
Shared controls / suppliers		
Benefit, cost and reliability		

CORRECTIVE ACTION

Cause / action	Owner / agreed target date	Verification / closure

PORTFOLIO READINESS DISCUSSION

- ☐ Controls have owners, evidence, and a review cadence.
- ☐ Independent findings lead to tracked and retested fixes.
- ☐ Portfolio risks and time-limited exceptions reach decision makers.
- ☐ Autonomous actions, where used, have enforceable limits.
- ☐ Management reviews change priorities, controls, or resources when needed.

An aggregate accuracy score cannot represent the whole risk picture. Verify whether corrective actions address the observed failure; update controls, evaluations and training as appropriate.

01 EVIDENCE

02 CHALLENGE

03 RISK

04 IMPROVE

05 RESOURCES

GOVERNING AI ACROSS AN ORGANIZATION

A useful resource shelf.

Use official guidance to define actions, responsibilities and evidence for your actual use case.

ISO/IEC 42001

Structure policies, responsibilities, operations, reviews, and continual improvement.

<https://www.iso.org/standard/81230.html>

NIST AI RMF

Build a shared risk language and a use-case risk record.

<https://www.nist.gov/itl/ai-risk-management-framework>

AI Controls Matrix v1.1

Assign shared control responsibilities and collect supplier or internal evidence.

<https://cloudsecurityalliance.org/artifacts/ai-controls-matrix-v1-1>

MITRE ATLAS

Threat-model your systems and plan adversarial control tests.

<https://atlas.mitre.org/>

OECD AI Principles

Translate your organization's AI values into policies and decision criteria.

<https://oecd.ai/en/ai-principles>

Access: ISO's overview is free; its full standard is paid. CSA downloads may require an account. Publisher material can change; follow the official pages for updates.

YOUR NEXT ACTION

Next evidence gap to close / owner / independent verification

Source notes: original worksheets adapted from the site's advanced working kit and AISM notebook themes. No source PDFs or paid study materials are reproduced. Official resource pages reviewed October 3, 2026. Starting, operating and advanced are editorial groupings, not a required sequence or a recognized maturity, safety, legal or certification assessment.