

OPERATING AI IN A BUSINESS PROCESS

Know what actually runs.

Connect each live deployment to an owner, release decision, operating controls and response plan. Adapt the depth of review to the consequences of failure.

Business process / users / affected people

Business and technical owners

Model, application and provider versions

Environment / integrations / permissions

Data sources, retrieval stores, provenance and permitted uses

SHARED CONTROLS AND DEPENDENCIES

Deployment / dependency	Control and owner	Coverage / evidence / gaps

MAKE COVERAGE EXPLICIT

A shared control needs an owner and evidence. Its existence does not prove a deployment is covered. Note when a provider controls updates or does not expose a stable version.

OPERATING AI IN A BUSINESS PROCESS

Give the release a gate.

Define release criteria before testing. Evaluate the whole workflow, including retrieval, interfaces, people and tools. Use representative tasks and realistic failure cases; general benchmark scores are insufficient for approving a specific business use.

Gate	Evidence / result and limits	Decision owner / criteria
Purpose and data rights		
Task performance vs. baseline		
Privacy and security		
Bias / accessibility / affected people		
Monitoring and fallback		
Residual risk and final approval		

TEST THE WORKFLOW, NOT ONLY THE MODEL

Where applicable, test prompt injection, manipulated retrieval, unsafe tool actions and disclosure. Record evaluation-set and subgroup coverage limits. Protect evaluation data and separate it from tuning where needed.

Material change that will trigger retesting / accountable approver

01 SYSTEM

02 RELEASE

03 SUPPLIER

04 RESPONSE

05 RESOURCES

OPERATING AI IN A BUSINESS PROCESS

Check the supplier relationship.

Provider claims and assurance reports are inputs to your decision. Verify that they cover the service, configuration and period you use; record the gaps you must address.

Supplier question	Answer / evidence	Owner / unresolved action
Retention, training use and subprocessors?		
Shared security and privacy controls?		
Change and incident communication?		
Usage rights, availability and support?		
Data removal and service replacement?		

Important supplier dependency / fallback or exit plan

KEEP THE RECORD CURRENT

Reassess when the service, terms, configuration or purpose changes. Your organization still owns the decisions and controls assigned to it, even when a provider delivers part of the system.

01 SYSTEM

02 RELEASE

03 SUPPLIER

04 RESPONSE

05 RESOURCES

OPERATING AI IN A BUSINESS PROCESS

Notice failures. Know who acts.

Combine user reports and sampled outcomes with service metrics. Define triggers from the actual task and risk decision, with named responders and feasible recovery actions.

Signal / failure	Trigger and responder	Fallback / recovery action
Quality deterioration		
Privacy / security / harmful output		
Provider outage or change		
Cost / latency / capacity		

Incident record: scope, containment, evidence

Recovery checks / communication owner

OPERATING READINESS DISCUSSION

- ☐ Every production use case has an owner and current system record.
- ☐ Release gates cover the risks of the actual task.
- ☐ Access, data, and output controls are enforced outside the model.
- ☐ Monitoring has thresholds, owners, and an escalation route.
- ☐ Fallbacks and supplier responsibilities have been tested or verified.

Protect sensitive logs. Identify who determines communication and applicable reporting obligations. Restore service after the responsible owner verifies recovery conditions.

01 SYSTEM

02 RELEASE

03 SUPPLIER

04 RESPONSE

05 RESOURCES

OPERATING AI IN A BUSINESS PROCESS

A useful resource shelf.

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

NIST AI RMF

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

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

OWASP LLM Top 10

Choose abuse cases and security tests for your application.

<https://genai.owasp.org/llm-top-10/>

MITRE ATLAS

Threat-model your systems and plan adversarial control tests.

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

AI Controls Matrix v1.1

Assign shared control responsibilities and collect supplier or internal evidence.

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

ISO/IEC 42001

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

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

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 control to verify / owner / evidence and review point

Source notes: original worksheets adapted from the site's operating 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.