

FinternetOps

Enterprise Governance Kit

AI & AgentOps for Regulated Financial Systems

Evidence. Explainability. Control.

What this kit is

A procurement-safe, audit-safe governance package for operating AI and agent systems in regulated financial environments.

Includes decision framework, operating model, templates, checklists, scenarios, and filled examples.

Endorsed by: MBCC (MoeCommunityCloud)

Version: 2026-01-13

Contents

- 1. Executive Governance Brief
- 1A. Executive Decision Table (Visual Wireframe)
- 2. Governance Operating Model
- 3. Evidence & Artifact Templates
- 4. AgentOps Control Checklist
- 5. Practical Governance Scenarios
- 6. Pilot & Adoption Guide
- Appendix A — Filled Evidence Pack Example
- Appendix B — Filled Governance Narrative Example
- Appendix C — Printable AgentOps Checklist
- Appendix D — Executive Approval & Sign-off Form

1. Executive Governance Brief

Purpose

Enable executive leadership to determine whether an AI/agent system can be operated, audited, and scaled without unacceptable risk.

The governance reality

Most enterprise AI initiatives fail after deployment because governance is missing: evidence trails, ownership clarity, drift prevention, and change control. FinternetOps treats agents as operational systems, not experiments.

Executive decision summary

Approve when...	Block / pause when...
Evidence packs and narratives are produced automatically.	Evidence must be reconstructed manually.
Ownership is explicit across Ops, Risk, Compliance.	Ownership is disputed or unclear.
Agent behavior is governed (specs, RBAC, versioning).	Agents drift silently or change without approval.
Stop/rollback authority is defined and tested.	No safe rollback or kill-switch exists.

1A. Executive Decision Table (Visual Wireframe)

Scan time ~60 seconds. Decide: Approve / Conditional / Block.

Operational Truth PASS: timestamped, attributable reality. FAIL: conflicting logs.	Evidence Generation PASS: artifacts by default. FAIL: manual reconstruction.
Explainability PASS: plain-English narrative. FAIL: technical outputs only.	Ownership PASS: named owners + escalation. FAIL: unclear responsibility.
Agent Control PASS: specs/guardrails/RBAC enforced. FAIL: unmanaged agents/drift.	Change Control PASS: approvals + versioning + rollback. FAIL: silent updates.
Monitoring PASS: actionable thresholds + routing. FAIL: alert noise.	Audit Readiness PASS: artifacts retrievable on demand. FAIL: scramble to prepare evidence.

2. Governance Operating Model

RACI, cadence, and authority boundaries.

Function / Artifact	Ops	Risk	Compliance	Executive
Agent Specification	R	C	I	A
Guardrail Definition	C	R	C	A
Monitoring Thresholds	R	C	I	A
Evidence Pack Review	I	C	R	A
Narrative Approval	I	C	R	A
Change Approval	R	C	C	A
Deployment / Scale	R	C	C	A
Stop / Rollback Authority	I	C	C	A

Cadence	Artifact	Audience
Real-time	Alerts & incidents	Ops
Daily	System health summary	Ops
Weekly	Governance brief	Exec + Risk
Monthly	Control & evidence review	Compliance
Quarterly	Stress scenarios & posture	Exec

3. Evidence & Artifact Templates

Copy/paste ready artifacts for audit and governance review.

Field	Value
Evidence Pack ID	AUTO-GENERATED
Event Classification	<input type="checkbox"/> Monitoring <input type="checkbox"/> Incident <input type="checkbox"/> Stress <input type="checkbox"/> Change Request
Timestamp (UTC)	
Source Agent + Version	
Impacted Process	
Severity	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High
Controls Executed	Guardrails <input type="checkbox"/> Pass/ <input type="checkbox"/> Fail RBAC <input type="checkbox"/> Pass/ <input type="checkbox"/> Fail Halt <input type="checkbox"/> Yes/ <input type="checkbox"/> No
Risk Snapshot	Exposure <input type="checkbox"/> Yes/ <input type="checkbox"/> No Residual <input type="checkbox"/> Acceptable/ <input type="checkbox"/> Elevated/ <input type="checkbox"/> Critical
Artifacts	log://... metric://... version hash config checksum

Governance Narrative (template)

1. What Happened — plain-English description.
2. Why It Matters — business/operational/regulatory relevance.
3. What Changed — actions taken.
4. Status — ☐ Resolved ☐ Ongoing ☐ Escalated
5. Required Action — ☐ None ☐ Monitor ☐ Approve Change ☐ Executive Decision
6. Next Review Date

4. AgentOps Control Checklist

Control Domain	Mandatory checks
Specification	Purpose, scope, inputs, outputs, escalation
Guardrails	Action limits, thresholds, fail-safe, kill switch
RBAC	Unique identity, least privilege, credential handling
Logging	Execution logs, decision context, metrics, routing
Change Control	Versioning, approvals, rollback, deployment record

Rule

Any mandatory failure blocks deployment, scaling, or white-label delivery.

5. Practical Governance Scenarios

Scenario	Trigger	Controls	Decision
Settlement exception	Delay exceeds tolerance	Halt + evidence + escalation	Exec approves resume/escalate
Liquidity stress	Scenario breaches threshold	Evidence + posture calc	Exec accepts/adjusts/suspend
Behavior drift	Output deviates from spec	Guardrails + block + rollback	Correct/rollback/decommission

6. Pilot & Adoption Guide

Phase	Scope	Outputs
Week 1 — Setup	Select 1–3 agents, approve specs, enable monitoring & logs	Baseline evidence + routing tests
Weeks 2–3 — Validate	Run supervised, generate evidence packs & narratives	Weekly governance review + remediation list
Week 4 — Executive Review	Review artifacts, posture, escalation effectiveness	Scale / adjust / stop decision

Appendix A — Filled Evidence Pack Example

Field	Value
Evidence Pack ID	EP-2026-01-SETTLE-0047
Event ID	EVT-SETTLE-0047
Timestamp (UTC)	2026-01-11 14:37:22
Source Agent	Settlement Monitoring Agent v1.3.2
Impacted Process	T+0 tokenized settlement — Counterparty C
Controls	Guardrails PASS; RBAC PASS; Halt YES; Escalation YES; Change Lock YES
Risk	Exposure YES; Impact <\$250,000; Residual Acceptable

Appendix B — Filled Governance Narrative Example

GN-2026-01-SETTLE-0047 (linked to **EP-2026-01-SETTLE-0047**)

What happened: Settlement latency exceeded tolerance for Counterparty C in a T+0 tokenized settlement flow involving Token ABC.

Why it matters: Prevents counterparty and liquidity exposure from compounding; preserves auditability.

What changed: Downstream halted; RBAC validated; evidence pack generated; escalated; change lock applied.

Status: Resolved. Executive approved resumption with heightened monitoring for 24 hours.

Appendix C — Printable AgentOps Checklist

Domain	Checks	Pass/Fail
Specification	Purpose, scope, inputs, outputs, escalation	<input type="checkbox"/> Pass <input type="checkbox"/> Fail
Guardrails	Limits, thresholds, fail-safe, kill switch	<input type="checkbox"/> Pass <input type="checkbox"/> Fail
RBAC	Identity, least privilege, credential handling	<input type="checkbox"/> Pass <input type="checkbox"/> Fail
Logging	Logs, decision context, metrics, routing	<input type="checkbox"/> Pass <input type="checkbox"/> Fail
Change	Versioning, approvals, rollback, record	<input type="checkbox"/> Pass <input type="checkbox"/> Fail

Appendix D — Executive Approval & Sign-off Form

Field	Value
Program / Initiative	<input type="text"/>
Agents + Versions	<input type="text"/>
Environment	<input type="checkbox"/> Prod <input type="checkbox"/> Staging <input type="checkbox"/> Test
Decision	<input type="checkbox"/> Approve <input type="checkbox"/> Approve w/ conditions <input type="checkbox"/> Block
Conditions / Notes	<input type="text"/>