CedarBridge Financial

# 07 | Controls and Evidence Matrix

Financial-services AI governance engagement

| | |
|---|---|
| Engagement type | Simulated portfolio case study |
| Organization | CedarBridge Financial, fictional mid-sized consumer lender and digital bank |
| Scope | Enterprise AI and model governance across credit, fraud, customer service, marketing, and operations |
| Primary scenario | CreditPath consumer credit underwriting model and ClearSignal fraud-AI vendor |

This artifact uses fictional systems and synthetic data. It is designed to show governance judgment, model-risk discipline, consumer-protection awareness, and operational evidence rather than to represent any real company or vendor.

## Purpose

This matrix translates AI and model-risk concerns into accountable controls and auditable evidence. It is designed to prevent the governance program from becoming a policy-only exercise.

## Controls and evidence matrix

| | | | | | | |
|---|---|---|---|---|---|---|
| R-001 | CreditPath produces disparate outcomes for a protected or proxy-vulnerable group. | Fair-lending/outcomes testing, feature restriction, alternative configuration review, legal sign-off. | Compliance + Model Risk | Fair-lending report, feature log, remediation memo | Quarterly and before material change | High |
| R-002 | CreditPath cannot provide specific and accurate adverse-action reasons. | Reason-code mapping, monthly QA sampling, complaint review, blocked launch if reason engine fails. | Credit Risk | Reason-code test results, QA log | Monthly | High |
| R-003 | Model performance degrades after economic or portfolio shift. | Calibration monitoring, PSI/drift thresholds, challenger model, rollback plan. | Model Owner | Monitoring dashboard, issue log | Monthly | Moderate |
| R-004 | Vendor fraud model changes without review. | Contractual change notice, vendor attestation, release-impact review. | Procurement + Fraud Ops | Vendor notice, change approval | Each change | Moderate |
| R-005 | LLM customer-service tool gives inaccurate regulated response. | Approved knowledge base, refusal rules, human escalation, QA sampling. | Customer Ops | QA sample, escalation logs | Weekly during pilot | Moderate |
| R-006 | Consumer data entered into unapproved GenAI. | Approved-tool policy, DLP, training, incident reporting. | Security + Privacy | DLP alerts, training records | Continuous / quarterly | Low |
| R-007 | Inventory misses AI embedded in vendor platforms. | Quarterly attestations, procurement intake AI screen, vendor feature review. | AI Governance Office | Attestation, intake records | Quarterly | Moderate |
| R-008 | Manual overrides are inconsistent or undocumented. | Override taxonomy, required reason capture, review sampling. | Credit Ops | Override log, QA review | Monthly | Moderate |
| R-009 | Thin-file applicants are unfairly disadvantaged. | Alternative documentation process, segment monitoring, model limitation disclosure internally. | Credit Risk | Manual review metrics, segment report | Monthly | High |
| R-010 | Fraud false positives create account access harm. | False-positive rate thresholds, dispute routing, customer-impact monitoring. | Fraud Ops | False-positive dashboard, complaints | Monthly | Moderate |
| R-011 | Third-party outage disrupts critical process. | Business continuity plan, fallback process, SLA monitoring. | Operations + Vendor Mgmt | BCP test, SLA report | Semiannual | Moderate |
| R-012 | Model documentation is stale or incomplete. | Annual owner attestation and document refresh workflow. | Model Risk | Attestation, document repository | Annual / change | Low |

## Evidence standards

- Evidence must be dated, retained, reviewable, and tied to a named control owner.
- For critical models, evidence must support independent validation and executive approval.
- Issue closure requires proof of remediation, not only a status note.
- Controls with stale evidence are reported as open gaps in the Executive Risk Committee pack.

## Testing approach

| | | |
|---|---|---|
| Preventive controls | Second line or control owner | Design review, checklist sampling, system configuration review. |
| Detective controls | Model Risk / Compliance / Security | Metric trend review, exception testing, log review, complaint sample. |
| Corrective controls | Issue owner with second-line challenge | Remediation evidence review, retest, residual-risk acceptance. |

| | | |
|---|---|---|
| Board-visible controls | AI Governance Office | Quarterly status and exceptions reporting. |

## Reference basis

This simulated package is informed by the 2026 Revised Guidance on Model Risk Management issued by the Federal Reserve, OCC, and FDIC, NIST AI RMF 1.0, the CFPB circular on adverse-action notices for complex credit algorithms, CFPB guidance on specificity of adverse-action reasons, and the 2023 interagency guidance on third-party relationships. These references are used as design inputs for a portfolio artifact, not as legal advice.