CedarBridge Financial

04 | Model Governance Standard

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 standard defines required lifecycle controls for model development, validation, implementation, use, monitoring, change management, and decommissioning. It applies to bank-owned models and third-party model outputs used in CedarBridge processes.

Lifecycle control requirements

Development	Document business purpose, conceptual design, target population, assumptions, intended output, known limitations, data source controls, feature approval, explainability method, and adverse-action reason strategy where relevant.	Model development document, data dictionary, feature log, explainability memo, limitation register.
Pre-implementation validation	Validate conceptual soundness, data quality, implementation quality, performance, sensitivity, limitations, outcomes, fair-lending/consumer impact, and user acceptance.	Independent validation report, remediation tracker, approval memo.
Implementation	Confirm production code, access controls, monitoring feeds, fallback process, user training, model-card publication, and issue logging.	Implementation checklist, release notes, access review, UAT sign-off.
Use	Define authorized users, permitted decisions, prohibited uses, override rules, output interpretation, human-review duties, and escalation path.	User guide, training log, override record template, control attestation.
Monitoring	Track performance, drift, stability, data quality, outcomes, fairness, complaints, overrides, incidents, and vendor changes.	Monitoring dashboard, monthly review minutes, issue log.
Material change	Classify changes and require retesting, approval, communication, and rollback plan.	Change request, test results, approval evidence, rollback evidence.
Decommissioning	Retire model safely, preserve records, disable feeds, confirm data retention/deletion, and notify impacted users.	Decommissioning checklist, archive, deletion certificate.

Minimum documentation package

- Model card or model risk assessment.
- Development and use documentation.
- Data and feature risk assessment.
- Validation report and limitation register.
- Implementation checklist and user guide.
- Monitoring plan with thresholds and issue management.
- Change log, approvals, and production release notes.
- Third-party due diligence and contract controls when vendor-supplied or vendor-enabled.

Independence and challenge

Model development	Data Science / Credit Risk	Model Risk Management
Fair-lending analysis	Credit Risk Analytics	Compliance / Fair Lending
Security and privacy review	Engineering / Product	Information Security / Privacy
Vendor review	Business owner / Procurement	Third-Party Risk, Legal, Security
Production approval	Business owner	AI Risk Committee / Executive Risk Committee by tier

Material-change triggers

New or materially revised data source	Data/feature review, privacy review, performance retest, fairness/outcomes check.

Model algorithm change or retraining outside approved cadence	Validation scope decision, back-testing, sensitivity analysis, deployment approval.
Expanded product, geography, customer segment, or channel	Reclassification, consumer-impact review, control update.
Performance degradation beyond threshold	Incident or issue review, root-cause analysis, remediation, possible pause.
Vendor version update	Vendor evidence review, change-impact assessment, production approval.

Credit decision explainability and adverse-action procedure

When a model contributes to a negative credit decision, the model owner must demonstrate that CedarBridge can produce specific, accurate, and consumer-understandable principal reasons. Generic references to proprietary scores or internal standards are not sufficient. Reason codes must be traceable to validated model drivers, reviewed for accuracy, and monitored through complaint and quality-assurance sampling.

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.