CedarBridge Financial

06 | Third-Party AI Vendor Due-Diligence Assessment

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.

Vendor and service

Vendor	ClearSignal Analytics, fictional fraud-detection provider
Product	FraudGuard transaction-risk model
Use case	Real-time fraud risk scoring for debit-card, ACH, and digital-wallet transactions.
Decision influence	High. Scores recommend step-up authentication, transaction hold, or fraud analyst review.
Customer impact	Possible payment friction, transaction delay, account access interruption, false positives, and complaint risk.
Current decision	Approved with conditions; contract addendum and monitoring integration required.

Due-diligence questionnaire and evidence

Model documentation	Model purpose, methodology, training population, feature categories, limitations, validation results.	Partial documentation provided; feature-level details redacted.	High
Data use restrictions	Contractual prohibition on secondary use of CedarBridge data, model training without approval, and resale.	Agrees to restriction; draft DPA pending.	Moderate
Bias / outcomes testing	False-positive and false-negative analysis by relevant customer segments where lawful and appropriate.	Aggregate performance only; no customer segment outcomes shared.	High
Security	SOC 2 Type II, encryption, access controls, incident-response process, vulnerability management.	SOC 2 provided; pen-test summary pending.	Moderate
Change management	Advance notice for model retraining, feature changes, threshold changes, and material degradation.	30-day notice proposed for material model changes; emergency changes after notice.	Moderate
Audit rights	CedarBridge and regulators may review relevant controls, model documentation, monitoring, and incident evidence.	Vendor accepts limited customer audit, regulator access unresolved.	High
Subcontractors	List of hosting, enrichment, and data-processing subprocessors.	Hosting listed; enrichment provider not yet documented.	Moderate
Exit plan	Data return/deletion, transition support, shadow scoring export, service continuity.	Basic plan provided.	Moderate

Vendor scorecard

Model transparency	20%	2	0.40	Insufficient for high-risk vendor model.
Performance and validation	20%	3	0.60	Aggregate performance acceptable; segment analysis missing.
Consumer-impact controls	15%	3	0.45	False-positive dispute path needs integration.
Data governance	15%	3	0.45	DPA and secondary-use restriction pending.
Security resilience	15%	4	0.60	Generally acceptable pending pen-test summary.
Change and incident notice	10%	3	0.30	Model-change notice requires tighter SLA.
Exit and portability	5%	3	0.15	Minimum plan present.
Total	100%	-	2.95 / 5	Conditional approval only.

Contract controls required before renewal

- Regulator and CedarBridge audit/access rights for high-risk controls and model evidence.

- Notice and approval process for material model changes, thresholds, data sources, and degradation events.
- Incident notice within 24 hours for data exposure, model failure, significant false-positive surge, service outage, or unauthorized data use.
- Contractual prohibition on secondary use of CedarBridge data for vendor training, enrichment, or resale without written approval.
- Right to export transaction-level scores, reason indicators, and monitoring data needed for validation and exit.
- Subcontractor disclosure, flow-down controls, and approval rights for critical subprocessors.

Approval decision

ClearSignal FraudGuard may continue under conditional approval for 90 days. Renewal is blocked unless the vendor completes audit-rights language, DPA execution, model-change controls, segment-level monitoring evidence, and a tested exit plan.

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.