AI Governance Framework — TechCorp Financial Services (Sample)

AI Governance Framework

Enterprise Policy & Control Structure

Organization: TechCorp Financial Services (Sample)

Industry: Financial Services — Digital Banking & Wealth Management

Prepared by: Elevated AI

Date: December 2025

Version: 1.0

Confidentiality: Sample Deliverable — Anonymized

Executive Summary

This AI Governance Framework establishes the policies, processes, and control structures required for TechCorp Financial Services to deploy artificial intelligence systems responsibly, ethically, and in compliance with applicable regulations. This framework addresses AI risk management, use case approval workflows, monitoring requirements, incident response protocols, and ongoing governance processes.

Framework Objectives:

1. Enable safe and responsible AI adoption across the enterprise
2. Ensure compliance with financial services regulations (FCRA, ECOA, SOX, etc.)
3. Manage AI-related risks including bias, privacy, security, and operational reliability
4. Establish clear accountability and decision-making authority for AI systems
5. Build stakeholder trust through transparent and ethical AI practices

Governance Scope:

This framework applies to all AI and machine learning systems used by TechCorp, including:

- Customer-facing applications (chatbots, recommendation engines, personalization)
- Internal operational systems (fraud detection, underwriting, portfolio management)

- Third-party AI services and vendor solutions
- Experimental and pilot AI projects

Table of Contents

---

1. Governance Structure & Roles

AI Governance Committee (AIGC)

Purpose: Provide executive oversight and strategic direction for AI adoption, ensuring alignment with business objectives, risk tolerance, and regulatory requirements.

Membership:

- **Chair:** Chief Risk Officer
- **Members:**
  - Chief Technology Officer
  - Chief Data Officer
  - Chief Compliance Officer
  - Chief Information Security Officer
  - Head of Legal
  - Head of Internal Audit

- Chief Marketing Officer
- Head of Customer Experience
- Representative from Lines of Business

Responsibilities:

- Approve AI strategy and investment priorities
- Review and approve high-risk AI use cases
- Set AI risk appetite and tolerance levels
- Oversee AI ethics and fairness standards
- Monitor enterprise-wide AI risk metrics
- Escalate significant AI issues to Board Risk Committee
- Quarterly governance reviews and annual strategy updates

Meeting Cadence: Monthly (plus ad-hoc for urgent matters)

AI Risk & Ethics Review Board (ARERB)

Purpose: Conduct detailed technical and ethical review of AI use cases, models, and deployments to ensure responsible and compliant implementation.

Membership:

- **Chair:** Chief Data Officer
- **Members:**
  - Data Science Leadership
  - Model Risk Management
  - Privacy Officer
  - Information Security
  - Legal/Compliance Representatives
  - Business Line Representatives (rotating)
  - External Ethics Advisor (optional)

Responsibilities:

- Review and approve all AI use case proposals
- Conduct fairness, bias, and ethics assessments
- Validate model risk ratings and mitigation plans

- Review pilot results and production readiness
- Monitor ongoing AI system performance
- Investigate AI-related incidents and recommend remediation
- Maintain AI use case registry and risk inventory

Meeting Cadence: Bi-weekly (plus ad-hoc for urgent reviews)

AI Center of Excellence (AI CoE)

Purpose: Provide technical expertise, standards, and enablement support for AI development and deployment across the enterprise.

Team Structure:

- **Lead:** Head of AI/ML Engineering
- **Core Team:**
  - AI/ML Engineers and Data Scientists
  - MLOps and Platform Engineers
  - AI Product Managers
  - Technical Writers and Trainers

Responsibilities:

- Develop and maintain AI development standards and best practices
- Provide technical consulting and architecture guidance for AI projects
- Build and operate shared AI platform and tooling
- Deliver training and enablement programs
- Maintain model registry and documentation repository
- Drive innovation through research and proof-of-concept projects
- Report technical metrics to ARERB and AIGC

Business Line AI Owners

Role: Accountable for AI systems deployed within their business domain, including business outcomes, customer impact, and operational performance.

Responsibilities:

- Define business requirements and success criteria for AI use cases
- Ensure adequate budget and resources for AI initiatives

- Monitor business performance and customer feedback
- Escalate issues and risks to ARERB and AIGC
- Participate in governance reviews for their AI systems

Model Developers & Data Scientists

Role: Design, develop, test, and document AI models in accordance with governance standards.

Responsibilities:

- Follow AI development standards and best practices
- Complete required documentation and risk assessments
- Conduct fairness and bias testing
- Submit models for validation and approval
- Participate in post-deployment monitoring and optimization
- Report anomalies and performance issues

---

2. AI Principles & Ethics Charter

TechCorp Financial Services is committed to developing and deploying AI systems that are **fair, transparent, accountable, secure, and beneficial** to our customers and society.

Core Principles

Principle 1: Fairness & Non-Discrimination

Commitment: AI systems shall not discriminate against individuals or groups based on protected characteristics including race, color, religion, national origin, sex, gender identity, sexual orientation, age, disability, or other legally protected status.

Implementation:

- Bias testing required for all customer-impacting AI models
- Regular fairness audits using demographic parity and equalized odds metrics
- Diverse training data and mitigation strategies for identified biases
- Human review for adverse decisions (credit denial, account closure, etc.)
- Transparent appeals process for customers

Principle 2: Transparency & Explainability

Commitment: Customers and stakeholders have the right to understand how AI systems impact decisions that affect them.

Implementation:

- Customer disclosure when interacting with AI systems (chatbots, voice agents)
- Explainable AI techniques for high-stakes decisions
- Adverse action notices include key decision factors
- Model documentation accessible to audit and compliance teams
- Plain-language explanations available to customers upon request

Principle 3: Accountability & Human Oversight

Commitment: Humans remain accountable for AI system outcomes. Clear lines of responsibility exist for every AI deployment.

Implementation:

- Business owner assigned to every production AI system
- Human-in-the-loop review for high-stakes or sensitive decisions
- Escalation protocols when AI confidence is low or outcomes are unusual
- Regular performance reviews by business owners and governance bodies
- Clear incident response and remediation processes

Principle 4: Privacy & Data Protection

Commitment: AI systems shall protect customer privacy and handle personal data in accordance with applicable laws and TechCorp policies.

Implementation:

- Privacy Impact Assessments required for all AI use cases
- Data minimization: collect and use only necessary data
- Consent obtained where required by law or policy
- Secure data handling and storage practices
- Right to deletion and data portability honored
- Third-party data sharing restricted and governed

Principle 5: Security & Robustness

Commitment: AI systems shall be secure, reliable, and resilient against adversarial attacks and operational failures.

Implementation:

- Security assessments required before production deployment
- Adversarial testing for critical models
- Input validation and anomaly detection
- Redundancy and failover mechanisms
- Continuous monitoring for drift and degradation
- Incident response plans for AI failures

Principle 6: Beneficial Purpose

Commitment: AI systems shall be developed and deployed to create value for customers, employees, and society while avoiding harm.

Implementation:

- Business case required demonstrating customer and/or operational benefit
- Risk-benefit analysis conducted for all use cases
- Customer feedback mechanisms and satisfaction monitoring
- Prohibition on AI use cases that cause unjustified harm
- Regular review of societal impact and alignment with corporate values

---

3. Risk Assessment Framework

AI Risk Taxonomy

TechCorp categorizes AI risks into six primary domains:

1. Regulatory & Compliance Risk

Description: Risk of violating laws, regulations, or industry standards governing financial services and data use.

Key Concerns:

- Fair lending laws (ECOA, FCRA)
- Anti-discrimination requirements
- Consumer protection regulations (CFPB oversight)
- Data privacy laws (GDPR, CCPA, state laws)
- Model risk management (SR 11-7 for banks)
- SOX controls for financial reporting

Mitigation Approaches:

- Compliance review integrated into use case approval
- Fairness testing and bias audits
- Documentation and audit trail requirements
- Legal counsel consultation for novel use cases

2. Fairness & Bias Risk

Description: Risk that AI systems produce discriminatory outcomes or perpetuate historical biases.

Key Concerns:

- Disparate impact on protected groups
- Proxy discrimination via correlated features
- Training data bias
- Measurement and label bias
- Feedback loops amplifying bias over time

Mitigation Approaches:

- Diverse and representative training data
- Bias detection metrics (demographic parity, equalized odds, etc.)
- Fairness constraints in model development
- Human review for sensitive decisions
- Regular bias audits and retraining

3. Privacy & Data Protection Risk

Description: Risk of unauthorized data access, use beyond consent, or privacy violations.

Key Concerns:

- Use of sensitive personal information
- Data minimization failures
- Inadequate consent or notice
- Third-party data sharing risks
- Re-identification of anonymized data
- Cross-border data transfer restrictions

Mitigation Approaches:

- Privacy Impact Assessments
- Data classification and access controls
- Encryption and anonymization techniques
- Consent management and audit trails
- Vendor data protection agreements

4. Operational & Performance Risk

Description: Risk that AI systems fail to perform as expected, degrade over time, or produce unreliable outputs.

Key Concerns:

- Model drift and degradation
- Distribution shift in input data
- Adversarial attacks and data poisoning
- System downtime and availability
- Incorrect predictions at scale
- Integration and dependency failures

Mitigation Approaches:

- Continuous monitoring and alerting
- Model retraining and validation cadence
- Anomaly detection and circuit breakers
- Redundancy and failover architecture
- Comprehensive testing before deployment

5. Reputational & Customer Trust Risk

Description: Risk that AI system behavior damages customer trust, brand reputation, or stakeholder confidence.

Key Concerns:

- Perception of unfairness or bias
- Opaque or "black box" decision-making
- Poor customer experience (e.g., unhelpful chatbot)
- Publicized incidents or failures

- Misalignment with customer expectations or values

Mitigation Approaches:

- Transparency and explainability practices
- Customer feedback loops and satisfaction monitoring
- Crisis communication and incident response plans
- Proactive disclosure and education
- Regular review of customer sentiment

6. Third-Party & Vendor Risk

Description: Risk arising from use of third-party AI services, models, or data providers.

Key Concerns:

- Vendor AI system quality and reliability
- Lack of visibility into vendor AI practices
- Vendor data security and privacy practices
- Vendor compliance with regulations
- Concentration risk and vendor lock-in
- Vendor business continuity

Mitigation Approaches:

- Vendor AI risk assessment and due diligence
- Contractual requirements for transparency and controls
- Regular vendor audits and performance reviews
- Alternative vendor identification
- Exit planning and data portability

AI Risk Rating Methodology

Every AI use case is assigned a risk rating based on a structured assessment of impact and likelihood across the six risk domains.

Risk Impact Assessment

Customer Impact Factors:

- Number of customers affected
- Sensitivity of decision (e.g., credit denial vs. product recommendation)

- Financial impact on customers
- Reversibility of decision
- Availability of human appeal

Business Impact Factors:

- Financial exposure (revenue, liability)
- Operational criticality
- Regulatory scrutiny level
- Reputational exposure
- Complexity of remediation

Impact Scoring (1-5 Scale)

Level 5 — Critical Impact:

- Affects >100,000 customers or entire customer base
- High-stakes decisions (credit approval, account closure, fraud accusation)
- Potential regulatory enforcement or class action liability
- Significant reputational risk if failure occurs
- Difficult or impossible to remediate at scale

Level 4 — High Impact:

- Affects 10,000-100,000 customers
- Moderate-stakes decisions with financial consequences
- Regulatory reporting or examination likely
- Measurable reputational harm from failure
- Complex remediation required

Level 3 — Moderate Impact:

- Affects 1,000-10,000 customers
- Low-stakes decisions with limited financial impact
- Regulatory interest possible but unlikely
- Limited reputational exposure
- Remediation feasible but resource-intensive

Level 2 — Low Impact:

- Affects <1,000 customers
- Minimal financial or decision consequences
- Limited regulatory relevance
- Minimal reputational risk
- Easy to remediate

Level 1 — Minimal Impact:

- Internal use only or very limited customer exposure
- No meaningful financial or decision impact
- No regulatory implications
- No reputational risk
- Trivial to remediate

Risk Likelihood Assessment

Likelihood Factors:

- Model complexity and interpretability
- Data quality and representativeness
- Maturity of technology and methods
- Testing and validation rigor
- Operational controls and monitoring
- Team experience and expertise

Likelihood Scoring (1-5 Scale)

Level 5 — Very High Likelihood:

- Novel or experimental techniques
- Poor data quality or limited training data
- Minimal testing or validation
- Weak or absent operational controls
- Inexperienced team

Level 4 — High Likelihood:

- Complex "black box" models
- Data quality concerns or bias identified

- Limited validation and testing
- Basic controls and monitoring
- Team has some AI experience

Level 3 — Moderate Likelihood:

- Moderately complex models with some interpretability
- Good data quality with minor gaps
- Standard validation and testing completed
- Adequate controls and monitoring
- Experienced team with AI expertise

Level 2 — Low Likelihood:

- Interpretable models or well-understood techniques
- High-quality, representative data
- Rigorous validation and testing
- Strong controls and comprehensive monitoring
- Highly experienced AI team

Level 1 — Very Low Likelihood:

- Simple, transparent models
- Exceptional data quality and coverage
- Extensive testing and validation
- Industry-leading controls and monitoring
- Expert team with deep domain knowledge

Overall Risk Rating Matrix

	Likelihood 1	**Likelihood 2**	**Likelihood 3**	**Likelihood 4**	**Likelihood 5**
Impact 5	High	High	Critical	Critical	Critical
Impact 4	Moderate	High	High	Critical	Critical
Impact 3	Low	Moderate	Moderate	High	High
Impact 2	Low	Low	Moderate	Moderate	High
Impact 1	Low	Low	Low	Low	Moderate

Risk Rating Definitions:

- **Critical Risk:** Requires AIGC approval, extensive testing, independent validation, continuous monitoring, quarterly reviews
- **High Risk:** Requires ARERB approval, rigorous testing, independent validation, continuous monitoring, semi-annual reviews
- **Moderate Risk:** Requires ARERB approval, standard testing and validation, regular monitoring, annual reviews
- **Low Risk:** Requires AI CoE approval, standard testing, periodic monitoring, biennial reviews

---

4. AI Use Case Approval Workflow

All AI use cases must follow a structured approval process before development, pilot, and production deployment.

Stage 1: Concept & Business Case

Objective: Validate business value and initial feasibility before significant investment.

Activities:

- Business owner completes AI Use Case Proposal template
- Define business problem, objectives, and success metrics
- Identify data sources and technical approach
- Estimate costs, timeline, and resources
- Conduct preliminary risk assessment (self-assessment)
- Submit to AI CoE for feasibility review

Approval Authority: AI CoE Lead

Deliverables:

- AI Use Case Proposal (completed template)
- Preliminary Risk Assessment
- Feasibility Recommendation from AI CoE

Decision: Approve to proceed to detailed design, request revisions, or decline

---

Stage 2: Detailed Design & Risk Assessment

Objective: Complete comprehensive risk assessment and design AI system architecture.

Activities:

- Detailed technical design and architecture documentation

- Data inventory and quality assessment
- Comprehensive risk assessment across all six domains
- Privacy Impact Assessment
- Bias and fairness analysis plan
- Security assessment and threat modeling
- Regulatory and compliance review
- Model validation plan
- Monitoring and alerting design
- Incident response plan
- Submit complete package to ARERB (or AIGC if Critical risk)

Approval Authority:

- **Low Risk:** AI CoE Lead
- **Moderate/High Risk:** AI Risk & Ethics Review Board
- **Critical Risk:** AI Governance Committee

Deliverables:

- Technical Design Document
- Comprehensive Risk Assessment
- Privacy Impact Assessment
- Security Assessment
- Compliance Review Memo
- Model Validation Plan
- Monitoring Plan
- Incident Response Plan

Decision: Approve to build, request revisions/additional controls, or decline

---

Stage 3: Development & Validation

Objective: Build, test, and validate AI model and system according to approved design.

Activities:

- Model development and training
- Bias and fairness testing

- Performance testing (accuracy, precision, recall, etc.)
- Security testing and vulnerability assessment
- Integration testing
- User acceptance testing (UAT)
- Independent model validation (for High/Critical risk)
- Documentation completion (model card, user guide, runbooks)
- Submit validation results to ARERB/AIGC

Approval Authority:

- **Low Risk:** AI CoE Lead
- **Moderate/High Risk:** ARERB
- **Critical Risk:** AIGC

Deliverables:

- Trained model and code
- Model Card (performance, fairness, limitations)
- Bias and Fairness Testing Report
- Validation Report (independent if High/Critical)
- UAT Results and Sign-off
- Complete Documentation Package

Decision: Approve to pilot, request additional testing, or decline

---

Stage 4: Pilot Deployment

Objective: Validate AI system performance in limited production environment with enhanced monitoring.

Activities:

- Deploy to pilot environment (limited user base or geography)
- Enhanced monitoring and logging
- Daily performance reviews
- Customer feedback collection
- Incident tracking and resolution
- Bias and fairness monitoring

- Pilot summary report and lessons learned
- Submit pilot results to ARERB/AIGC

Pilot Duration:

- **Low Risk:** 2-4 weeks
- **Moderate Risk:** 4-8 weeks
- **High Risk:** 8-12 weeks
- **Critical Risk:** 12+ weeks

Approval Authority: Same as Stage 3

Deliverables:

- Pilot Summary Report
- Performance Metrics vs. Success Criteria
- Bias and Fairness Monitoring Results
- Customer Feedback Summary
- Incident Log and Resolutions
- Production Readiness Checklist

Decision: Approve to production, extend pilot with modifications, or decline

---

Stage 5: Production Deployment

Objective: Deploy AI system to full production with appropriate controls and ongoing governance.

Activities:

- Full production deployment
- Activate monitoring dashboards and alerting
- Register in AI Use Case Registry
- Schedule ongoing governance reviews
- Communicate to stakeholders and users
- Begin regular performance reporting

Approval Authority: Business Line AI Owner (final deployment authorization)

Deliverables:

- Production deployment confirmation

- AI Use Case Registry entry
- Governance review schedule
- Monitoring dashboard and alert configuration
- Stakeholder communication materials

Ongoing Requirements:

- Continuous monitoring and alerting
- Regular performance reviews per risk rating
- Annual risk reassessment
- Model retraining and revalidation per schedule
- Incident reporting and remediation

---

5. Data Governance for AI

Data Quality Standards

AI models are only as good as the data they're trained on. TechCorp requires adherence to data quality standards for all AI use cases.

Accuracy: Data must be correct and free from errors. Validation rules and data quality checks required.

Completeness: Data must be sufficiently complete for intended AI use. Missing data patterns analyzed and addressed.

Consistency: Data must be consistent across sources and over time. Data lineage and transformation documented.

Timeliness: Data must be current and updated per requirements. Stale data policies enforced.

Representativeness: Training data must represent the population the AI will serve. Demographic analysis required for customer-facing models.

Data Quality Assessment: Required deliverable for all AI projects, documenting data quality across these dimensions and remediation plans for identified gaps.

Data Privacy & Protection

Data Minimization: Collect and use only data necessary for the AI use case. Justification required for sensitive data elements.

Consent & Notice: Customer consent obtained where required. Clear notice provided when AI systems use personal data.

Purpose Limitation: Data used only for approved AI purposes. Separate consent required for new uses.

Access Controls: Role-based access controls enforced. Data access logged and audited.

Retention & Deletion: Data retained only as long as needed. Automated deletion per retention policies.

Anonymization & De-identification: Applied where feasible to reduce risk. Re-identification testing performed.

Privacy Impact Assessment (PIA): Required for all AI use cases involving personal data. Reviews data flows, risks, and mitigation measures.

Training Data Documentation

All AI models require comprehensive training data documentation:

Data Sources: Complete list of data sources, including internal databases, third-party providers, and public datasets.

Data Lineage: Upstream systems and transformations applied.

Data Dictionary: Definition of all features/variables used.

Demographic Analysis: For customer-facing models, analysis of representation across protected groups.

Bias Assessment: Known biases or limitations in training data.

Date Range: Time period of training data.

Refresh Cadence: How often training data is updated.

Known Limitations: Missing populations, sparse data regions, data quality issues.

---

6. Model Development & Validation Standards

Model Development Best Practices

TechCorp requires adherence to industry best practices for AI model development:

Baseline Establishment: Simple baseline models established before complex approaches. Performance improvement justified.

Feature Engineering: Features documented with business rationale. Prohibited features identified (e.g., protected characteristics unless legally required).

Model Selection: Multiple model types considered. Selection justified based on performance, interpretability, and operational requirements.

Hyperparameter Tuning: Systematic approach to hyperparameter selection. Overfitting prevention measures applied.

Cross-Validation: Appropriate cross-validation techniques used. Hold-out test set maintained for final evaluation.

Performance Metrics: Comprehensive evaluation across relevant metrics (accuracy, precision, recall, AUC, etc.). Business-relevant metrics defined.

Fairness Testing: Bias and fairness metrics computed across demographic groups. Disparate impact analysis conducted.

Interpretability: Explainability techniques applied (SHAP, LIME, etc.). Key drivers of predictions documented.

Model Validation Requirements

Validation rigor scales with risk rating:

Low Risk Models:

- Developer testing and documentation
- Peer review by AI CoE
- Standard performance evaluation

Moderate Risk Models:

- Independent validation by Model Risk Management team
- Comprehensive performance testing
- Bias and fairness testing
- Sensitivity analysis
- Documentation review

High & Critical Risk Models:

- Independent validation by external third party or Model Risk Management
- Extensive performance testing across scenarios
- Rigorous bias and fairness testing with demographic analysis
- Sensitivity and stress testing
- Adversarial testing
- Comprehensive documentation review
- Benchmarking against alternative approaches

Validation Reports: Required for all Moderate/High/Critical models, documenting validation methodology, findings, limitations, and recommendations.

Model Documentation: Model Cards

Every production AI model requires a Model Card documenting:

Model Details:

- Model type and version
- Training date and data sources
- Developer and owner
- Intended use and business purpose

Performance:

- Overall performance metrics
- Performance across demographic groups (if applicable)
- Known limitations and failure modes
- Confidence intervals and uncertainty quantification

Fairness & Bias:

- Bias testing results
- Fairness metrics across protected groups
- Mitigation measures applied
- Residual bias and ongoing monitoring approach

Training Data:

- Data sources and date range
- Data volume and representativeness
- Known data quality issues or biases
- Prohibited features excluded

Ethical Considerations:

- Potential harms and mitigation measures
- Stakeholder impacts considered
- Alignment with AI principles

Operational Details:

- Input/output specifications
- Latency and throughput requirements
- Monitoring and retraining schedule

- Incident response contacts

---

7. Monitoring & Performance Management

Continuous Monitoring Requirements

All production AI systems require continuous monitoring across four dimensions:

1. Operational Performance Monitoring

Metrics:

- System availability and uptime
- Response time and latency
- Throughput and capacity utilization
- Error rates and failure modes
- Dependency health (upstream/downstream systems)

Alerting:

- Real-time alerts for outages or degraded performance
- Escalation procedures for critical systems
- Automated circuit breakers for severe failures

2. Model Performance Monitoring

Metrics:

- Prediction accuracy and error rates
- Confidence score distributions
- Feature distributions and drift detection
- Comparison to baseline/benchmark models
- Performance across customer segments

Alerting:

- Alerts for performance degradation below thresholds
- Alerts for significant distribution shift
- Alerts for unusual confidence patterns

3. Fairness & Bias Monitoring

Metrics:

- Fairness metrics across protected groups (demographic parity, equalized odds, etc.)
- Adverse action rates by demographic group
- Customer feedback and complaints related to fairness
- Appeal rates and overturn rates by group

Alerting:

- Alerts for statistically significant disparate impact
- Alerts for fairness metric degradation
- Escalation to ARERB for fairness concerns

4. Business Outcome Monitoring

Metrics:

- Business KPIs and success metrics defined in use case approval
- Customer satisfaction and NPS
- Revenue/cost impact
- Operational efficiency metrics
- Unintended consequences or side effects

Alerting:

- Alerts for failure to meet success criteria
- Alerts for negative customer feedback trends
- Escalation to Business Line AI Owner

Performance Review Cadence

Regular performance reviews ensure ongoing AI system health:

Daily (Critical Risk Models):

- Operational health dashboard review
- Anomaly investigation
- Incident log review

Weekly (High Risk Models):

- Performance metrics review
- Incident and alert summary
- Customer feedback review

Monthly (Moderate Risk Models):

- Comprehensive performance report
- Bias and fairness metrics review
- Business outcome assessment
- Continuous improvement backlog prioritization

Quarterly (All Models):

- Formal governance review by ARERB/AIGC
- Risk rating reassessment
- Strategic performance vs. objectives
- Retraining and enhancement planning

Annually (All Models):

- Comprehensive model validation and audit
- Risk assessment refresh
- Documentation updates
- Governance review by AIGC

Model Retraining & Refresh

AI models require periodic retraining to maintain performance:

Retraining Triggers:

- **Time-based:** Scheduled retraining per risk rating (quarterly for Critical/High, semi-annually for Moderate, annually for Low)
- **Performance-based:** Retraining triggered by performance degradation alerts
- **Data-based:** Retraining triggered by significant data distribution shifts
- **Business-based:** Retraining triggered by changes in business rules or objectives

Retraining Process:

1. Update training data with recent observations
2. Retrain model using approved methodology
3. Validate retrained model performance
4. Conduct A/B test of current vs. retrained model
5. Approve and deploy retrained model if improved

6. Update model card and documentation

Retraining Approval: Follows same approval authority as original model (AI CoE for Low, ARERB for Moderate/High, AIGC for Critical).

---

8. Incident Response & Remediation

AI Incident Definition

An **AI Incident** is any event involving an AI system that:

- Causes or has potential to cause customer harm or adverse impact
- Violates laws, regulations, or TechCorp policies
- Results in system failure or unavailability
- Exhibits bias or fairness concerns
- Generates significant customer complaints or negative feedback
- Attracts regulatory or media attention

Incident Severity Classification

Severity 1 — Critical:

- Significant customer harm or potential class action exposure
- Regulatory violation with enforcement risk
- Discrimination or bias causing adverse impact on protected groups
- Major system failure affecting large customer population
- Imminent or active media/regulatory scrutiny

Response: Immediate escalation to AIGC Chair and CRO. System may be taken offline pending investigation.

Severity 2 — High:

- Moderate customer harm or individual liability exposure
- Potential regulatory concern
- Identified bias or fairness issue requiring investigation
- System failure affecting significant but limited customer population
- Customer complaints indicating pattern of concern

Response: Escalation to ARERB within 4 hours. Enhanced monitoring and investigation initiated.

Severity 3 — Moderate:

- Minor customer inconvenience
- Policy violation or deviation from standards
- Performance degradation or anomalous behavior
- Isolated customer complaints
- Potential issue requiring investigation

Response: Reported to Business Line AI Owner and AI CoE. Investigation and remediation planned.

Severity 4 — Low:

- No customer impact
- Minor operational issue or bug
- Documentation or process deviation

Response: Logged and addressed in normal course of operations.

Incident Response Process

Step 1: Detection & Reporting

Detection Sources:

- Automated monitoring alerts
- Customer complaints or feedback
- Employee observations
- Audit findings
- Regulatory inquiries
- Media reports

Reporting: Any employee observing an AI incident must report immediately to:

- Business Line AI Owner
- AI CoE
- Compliance (for regulatory issues)
- Legal (for liability concerns)

Step 2: Initial Assessment & Escalation

Activities:

- Assess incident severity
- Determine immediate containment actions
- Escalate per severity protocols
- Activate incident response team
- Preserve evidence and logs

Decision: Determine whether to:

- Take system offline immediately
- Activate circuit breakers or fallback logic
- Continue operation with enhanced monitoring
- Implement immediate workaround

Step 3: Investigation & Root Cause Analysis

Activities:

- Assemble cross-functional investigation team
- Review system logs, predictions, and monitoring data
- Interview stakeholders and users
- Conduct technical analysis of model behavior
- Identify root cause(s)
- Assess scope and impact
- Document findings

Deliverable: Incident Investigation Report documenting timeline, root cause, impact, and preliminary recommendations.

Step 4: Remediation & Corrective Action

Activities:

- Develop remediation plan
- Implement fixes (code, model, data, or process)
- Test and validate fixes
- Deploy corrective actions
- Customer remediation if applicable (notifications, compensation, appeals)
- Update documentation and training materials

Approval: Remediation plan approved by ARERB or AIGC depending on severity.

Step 5: Post-Incident Review & Learning

Activities:

- Conduct post-mortem with all stakeholders
- Identify systemic issues or patterns
- Update governance framework, policies, or standards
- Share lessons learned across AI CoE and development teams
- Implement preventive measures for future incidents
- Update risk assessments and monitoring

Deliverable: Post-Incident Review Report with lessons learned and action items.

Customer Remediation Protocols

When AI incidents cause customer harm:

Notification: Affected customers notified promptly and transparently about issue, impact, and remediation.

Appeals: Clear appeals process provided for adverse decisions. Human review of appealed cases.

Compensation: Financial remediation provided where appropriate (fee waivers, compensation, restoration of benefits).

Systemic Review: All similar cases reviewed to identify additional affected customers.

Regulatory Reporting: Incidents reported to regulators per applicable requirements (e.g., data breaches, fair lending violations).

---

9. Third-Party AI Vendor Management

Vendor AI Risk Assessment

Third-party AI vendors require due diligence before engagement:

Vendor Questionnaire: Standardized questionnaire assessing:

- AI model architecture and training methodology
- Data sources and quality controls
- Bias testing and fairness measures
- Security and privacy practices

- Regulatory compliance
- Incident history and response protocols
- Documentation and transparency
- Service level agreements and support

Vendor Risk Rating: Vendors assigned risk rating using same methodology as internal AI use cases.

Approval Authority:

- **Low/Moderate Risk:** Procurement with AI CoE review
- **High Risk:** ARERB approval required
- **Critical Risk:** AIGC approval required

Contractual Requirements

Vendor agreements for AI services must include:

Transparency: Vendor must provide documentation of AI system capabilities, limitations, performance, and fairness.

Data Protection: Vendor must comply with TechCorp data privacy and security requirements. Data usage restrictions enforced.

Bias & Fairness: Vendor must conduct bias testing and provide fairness metrics. Ongoing monitoring required.

Compliance: Vendor must comply with financial services regulations applicable to TechCorp's use case.

Audit Rights: TechCorp retains right to audit vendor AI systems and practices.

Incident Response: Vendor must promptly notify TechCorp of AI incidents. Joint incident response protocols established.

Exit Planning: Data portability and transition assistance provisions included.

Ongoing Vendor Monitoring

Performance Monitoring: Vendor AI system performance continuously monitored by TechCorp.

Quarterly Business Reviews: Vendor performance, incidents, and roadmap discussed quarterly.

Annual Audits: High/Critical risk vendors audited annually.

Incident Tracking: Vendor-related incidents logged and trended.

Alternative Evaluation: Alternative vendors periodically evaluated to avoid lock-in.

10. Compliance & Regulatory Mapping

Applicable Regulations

TechCorp AI systems must comply with:

Federal Regulations

Fair Credit Reporting Act (FCRA)

- Applies to: AI models used in credit decisioning
- Requirements: Accuracy, adverse action notices, consumer rights to dispute and correct
- Governance Alignment: Model validation, explainability, adverse action procedures

Equal Credit Opportunity Act (ECOA) & Regulation B

- Applies to: AI models used in credit decisioning
- Requirements: Prohibition on discrimination based on protected characteristics
- Governance Alignment: Bias testing, fairness metrics, demographic analysis, disparate impact assessment

Fair Lending Laws (FHA, ECOA)

- Applies to: AI models used in lending and credit products
- Requirements: Fair treatment of protected classes, prohibition on disparate impact
- Governance Alignment: Fairness testing, ongoing bias monitoring, adverse action analysis

Gramm-Leach-Bliley Act (GLBA)

- Applies to: AI systems using customer financial information
- Requirements: Privacy notices, data security safeguards, opt-out rights
- Governance Alignment: Privacy Impact Assessments, data security controls, consent management

Bank Secrecy Act (BSA) & Anti-Money Laundering (AML)

- Applies to: AI systems for transaction monitoring and fraud detection
- Requirements: Effective monitoring, suspicious activity reporting, recordkeeping
- Governance Alignment: Model validation, monitoring, audit trails, incident reporting

Consumer Financial Protection Bureau (CFPB) Oversight

- Applies to: Consumer-facing AI systems

- Requirements: Fair, transparent, and non-discriminatory practices
- Governance Alignment: Comprehensive governance framework, fairness testing, consumer remediation

Sarbanes-Oxley Act (SOX)

- Applies to: AI systems affecting financial reporting
- Requirements: Internal controls, accuracy, auditability
- Governance Alignment: Model validation, documentation, change management, access controls

Model Risk Management — SR 11-7 (for regulated banks)

- Applies to: AI/ML models used in risk management and decision-making
- Requirements: Model development, validation, governance, ongoing monitoring
- Governance Alignment: Full governance framework aligns with SR 11-7 principles

State & International Regulations

California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)

- Requirements: Consumer rights to access, delete, opt-out; data minimization
- Governance Alignment: Privacy Impact Assessments, consent management, data retention policies

EU General Data Protection Regulation (GDPR)

- Applies to: EU customer data
- Requirements: Lawful basis, data minimization, right to explanation, data protection impact assessments
- Governance Alignment: Privacy Impact Assessments, explainability, consent management

EU AI Act (Proposed)

- Requirements: High-risk AI systems require conformity assessment, transparency, human oversight, robustness
- Governance Alignment: Risk-based governance framework, transparency measures, ongoing monitoring

State AI Bias and Fairness Laws (Emerging)

- Various states considering legislation on AI fairness and transparency
- Governance Alignment: Proactive fairness testing and transparency measures exceed current requirements

---

Compliance Mapping to Governance Controls

Regulation	Requirement	Governance Control
ECOA/Reg B	Prohibition on discrimination	Bias testing, fairness metrics, demographic analysis
FCRA	Adverse action notices	Explainability, adverse action procedures
GLBA	Privacy and data security	Privacy Impact Assessments, data security controls
SOX	Internal controls	Model validation, documentation, change management
SR 11-7	Model risk management	Full governance framework, validation, ongoing monitoring
CCPA/CPRA	Consumer data rights	Privacy controls, consent management, data retention
GDPR	Right to explanation	Explainability techniques, transparency documentation
CFPB Oversight	Fair and transparent practices	Comprehensive governance framework, customer remediation

11. Training & Awareness

AI Literacy Program

Target Audience: All employees

Curriculum:

- Introduction to AI and Machine Learning (basics)
- AI at TechCorp: Strategy and Use Cases
- AI Ethics and Responsible AI Principles
- AI Governance Framework Overview
- Reporting AI Incidents and Concerns

Delivery: Annual online training module (60 minutes)

Role-Based Training

For Data Scientists & AI Developers:

- AI Development Standards and Best Practices (8 hours)
- Bias Detection and Mitigation Techniques (4 hours)
- Explainability and Interpretability Methods (4 hours)
- Model Documentation and Model Cards (2 hours)
- AI Use Case Approval Process (2 hours)

- Privacy and Security for AI (4 hours)

For Business Line AI Owners:

- AI Governance Framework Deep Dive (4 hours)
- AI Risk Assessment and Management (4 hours)
- AI Business Case Development (2 hours)
- Ongoing Monitoring and Performance Management (2 hours)
- Incident Response and Remediation (2 hours)

For Compliance, Legal, Audit:

- AI Regulatory Landscape (4 hours)
- AI Fairness and Bias Assessment (4 hours)
- AI Auditing Techniques (4 hours)
- AI Governance Framework and Oversight (4 hours)

For Executives (AIGC Members):

- AI Strategy and Business Value (2 hours)
- AI Governance and Risk Management Executive Overview (2 hours)
- AI Ethics and Responsible AI Leadership (2 hours)
- AI Regulatory and Reputational Risk (2 hours)

Awareness Campaigns

Quarterly AI Governance Newsletter: Highlighting governance updates, lessons learned from incidents, new use cases, and best practices.

Lunch & Learn Sessions: Monthly sessions on AI topics (open to all employees).

AI Ethics Week: Annual awareness campaign with workshops, speaker series, and interactive activities.

AI Champions Network: Cross-functional community of practice for AI practitioners to share knowledge and collaborate.

---

12. Continuous Improvement

Framework Review & Updates

This governance framework is a living document, subject to regular review and updates:

Annual Review: AIGC conducts comprehensive annual review of governance framework, incorporating:

- Lessons learned from AI incidents
- Regulatory and legal developments
- Industry best practices and emerging standards
- Internal audit findings
- Stakeholder feedback

Ad-Hoc Updates: Framework updated as needed in response to:

- Significant AI incidents or failures
- New regulations or regulatory guidance
- Major strategic shifts in AI adoption
- Material changes in risk environment

Version Control: All framework updates versioned, approved by AIGC, and communicated to stakeholders.

Metrics & KPIs

AIGC monitors enterprise-wide AI governance health through KPIs:

AI Portfolio Metrics:

- Number of active AI use cases by risk rating
- Total investment in AI initiatives
- Business value delivered (ROI, cost savings, revenue)

Governance Process Metrics:

- Use case approval cycle time
- Approval/decline rates by stage
- Governance review completion rates

Risk & Compliance Metrics:

- Number of AI incidents by severity
- Mean time to resolution for incidents
- Audit findings related to AI
- Regulatory inquiries related to AI

Fairness & Bias Metrics:

- Number of models with identified bias issues
- Time to remediate bias concerns
- Customer complaints related to fairness
- Disparate impact metrics across portfolio

Performance Metrics:

- Model performance vs. baseline
- Model drift and degradation incidents
- Retraining cycle adherence
- Business outcome achievement rates

Training & Awareness Metrics:

- Training completion rates
- AI literacy assessment scores
- Engagement in awareness campaigns

Benchmarking & Industry Engagement

TechCorp actively participates in industry AI governance initiatives:

Industry Working Groups: Participation in financial services AI governance forums and consortia.

Regulatory Engagement: Proactive engagement with regulators on AI governance topics.

Peer Benchmarking: Regular benchmarking of governance practices against peer institutions.

Academic Collaboration: Partnerships with research institutions on responsible AI.

Thought Leadership: Publishing and presenting on AI governance best practices.

Appendix A: Templates & Tools

The following templates support governance framework execution:

AI Use Case Proposal Template: Structured format for submitting new AI use cases for approval.

Risk Assessment Template: Comprehensive risk assessment across six domains.

Privacy Impact Assessment Template: Structured PIA for AI use cases involving personal data.

Model Card Template: Standardized documentation for AI models.

Incident Report Template: Structured format for reporting and documenting AI incidents.

Vendor AI Assessment Questionnaire: Due diligence questionnaire for third-party AI vendors.

Monitoring Dashboard Templates: Pre-built monitoring dashboards for common AI use cases.

Templates available in TechCorp AI Governance SharePoint repository.

Appendix B: Definitions & Glossary

Artificial Intelligence (AI): Computer systems capable of performing tasks that typically require human intelligence, including learning, reasoning, problem-solving, perception, and language understanding.

Machine Learning (ML): Subset of AI focused on algorithms that learn patterns from data and improve performance without explicit programming.

Bias: Systematic and unfair discrimination against certain individuals or groups in favor of others. In AI, bias often arises from training data, model design, or deployment context.

Fairness: The principle that AI systems should treat individuals and groups equitably, without discrimination based on protected characteristics.

Explainability: The degree to which the internal mechanics and decisions of an AI system can be understood and explained to humans.

Model Drift: Degradation in model performance over time as the statistical properties of input data change.

Disparate Impact: When a facially neutral policy or practice disproportionately affects a protected group, even without intentional discrimination.

Protected Characteristics: Individual attributes protected from discrimination by law, including race, color, religion, national origin, sex, age, disability, and others.

Adverse Action: A negative decision affecting an individual, such as denial of credit, that triggers notification and explanation requirements.

Appendix C: Roles & Responsibilities Summary

Role	Key Responsibilities
AI Governance Committee	Executive oversight, strategy approval, risk appetite, high-risk use case approval
AI Risk & Ethics Review Board	Detailed use case review, fairness assessment, ongoing monitoring, incident investigation
AI Center of Excellence	Technical standards, platform, training, consulting, innovation
Business Line AI Owner	Business accountability, budget, performance monitoring, issue escalation

Role	Key Responsibilities
Model Developers	Development, testing, documentation, ongoing support
Model Risk Management	Independent validation, audit, risk assessment
Compliance	Regulatory mapping, compliance review, audit participation
Privacy Office	Privacy Impact Assessments, consent management, data protection
Information Security	Security assessments, threat modeling, vulnerability testing
Legal	Legal review, regulatory engagement, incident response support
Internal Audit	Independent governance audits, control testing

Conclusion

This AI Governance Framework provides TechCorp Financial Services with a comprehensive, risk-based approach to responsible AI adoption. By establishing clear policies, processes, and accountability structures, TechCorp can deploy AI systems confidently while managing risks and maintaining stakeholder trust.

Successful governance requires ongoing commitment, continuous improvement, and cross-functional collaboration. This framework is a living document that will evolve with TechCorp's AI journey, regulatory developments, and industry best practices.

Framework Owner:

Chief Risk Officer

For questions or governance support:

AI Center of Excellence

ai-governance@techcorpfinancial.com

Prepared by:

Elevated AI

johnathan@elevatedai.co

elevatedai.co

This is a sample deliverable demonstrating Elevated AI's methodology and deliverable quality. All company names, data, and specifics are fictional for illustrative purposes.