Back to Document Index

Model Governance Framework

Business Analysis Template for AI Projects

Template ID:	6.2
Category:	AI Governance, Risk & Compliance
Version:	1.0
Last Updated:	January 2026
Prerequisites:	AI Opportunity Assessment (1.1) High-Level AI Solution Architecture (1.3) AI Risk Assessment Report (6.1)

1. Document Purpose

This Model Governance Framework establishes the organizational structure, policies, processes, and controls for governing AI/ML models throughout their entire lifecycle—from development through retirement. Effective model governance ensures AI systems are developed responsibly, deployed safely, monitored continuously, and maintained in alignment with business objectives, regulatory requirements, and ethical principles.

Key purposes of this framework include:

- Define clear roles, responsibilities, and accountability for model governance
- Establish standardized processes for model development, validation, approval, and deployment
- Create model risk tiering system to apply appropriate oversight based on risk level
- Ensure comprehensive model documentation and inventory management
- Implement robust model monitoring and performance management processes
- Define change management and version control procedures for model updates
- Establish model retirement and decommissioning protocols
- Support regulatory compliance (AI Act, model risk management standards, industry regulations)
- Enable effective escalation and issue resolution for model-related concerns
- Create audit trail demonstrating responsible AI model management

Back to Document Index

2. When to Use This Template

Implement this Model Governance Framework when establishing or enhancing AI/ML governance capabilities. The framework should be adopted enterprise-wide and applied consistently across all AI initiatives.

Ideal Use Cases:

Launching AI Program: Establish governance foundation before deploying first production AI model to ensure responsible development from the start.

Scaling AI Initiatives: Formalize governance as AI adoption grows from pilot projects to enterprise-wide deployment across multiple use cases.

Regulatory Compliance: Implement governance framework to meet emerging AI regulations (EU AI Act, industry standards, model risk management requirements).

Risk Management: Create structured oversight to identify, assess, and mitigate risks associated with AI model deployment and operation.

Post-Incident Response: Strengthen governance after AI-related incidents or failures to prevent recurrence through better controls.

Merger/Acquisition: Establish unified governance when integrating AI capabilities from acquired companies or consolidating practices.

Audit Preparation: Document governance processes and controls to demonstrate responsible AI management to internal/external auditors.

Stakeholder Assurance: Provide transparency and accountability to executives, boards, regulators, and customers about AI oversight.

Model Portfolio Growth: Systematize governance as an organization manages an increasing number of models requiring consistent oversight.

Enterprise Transformation: Embed AI governance into broader digital transformation or data governance initiatives.

Back to Document Index

3. Model Governance Operating Model

Effective model governance requires clear organizational structure with defined roles, responsibilities, and decision-making authority. This operating model establishes the "who" of model governance.

Three Lines of Defense Model

Model governance follows the "three lines of defense" model from enterprise risk management:

First Line (Model Owners & Developers): Own and manage models day-to-day. Responsible for model development, testing, documentation, monitoring, and maintenance. Implement controls and comply with governance policies. Examples: Data Science teams, ML Engineering, Business Analytics.

Second Line (Model Risk & Governance): Provide independent oversight, challenge, and guidance. Define governance policies, perform model validation, assess risks, monitor compliance. Do not build models but ensure they meet standards. Examples: Model Risk Management, AI Governance Office, Compliance.

Third Line (Internal Audit): Provide independent assurance that first and second lines are effective. Audit governance processes, test controls, report to board/audit committee. Examples: Internal Audit, Risk Audit.

Key Governance Roles

AI Governance Committee (Executive Level)

Purpose: Strategic oversight and approval authority for AI program

Composition: Chief Data/Analytics Officer (Chair), CTO, CIO, Chief Risk Officer, General Counsel, Chief Compliance Officer, Business Unit Leaders

Responsibilities:
- Approve AI governance framework and policies
- Review and approve high-risk models before deployment
- Oversee AI strategy alignment with business objectives
- Monitor AI portfolio performance and risk exposure
- Resolve escalated governance issues
- Ensure adequate resources for responsible AI practices

Meeting Frequency: Quarterly (or monthly during high-activity periods)

Back to Document Index

Model Risk Committee (Operational Level)

Purpose: Day-to-day governance and operational oversight of model lifecycle

Composition: Model Risk Manager (Chair), AI/ML Engineering Lead, Data Science Lead, Model Validation Lead, Compliance Representative, Legal Representative

Responsibilities:
- Review and approve medium-risk models for deployment
- Monitor model performance and risks across portfolio
- Assess model validation findings and approve remediation plans
- Escalate high-risk models or issues to AI Governance Committee
- Track compliance with model governance policies
- Review model inventory and lifecycle status

Meeting Frequency: Bi-weekly or monthly

Chief AI/ML Officer (or equivalent)

Purpose: Executive accountability for AI model program

Responsibilities:
- Overall accountability for AI model governance framework
- Chair AI Governance Committee
- Ensure alignment between AI strategy and governance
- Allocate resources for model development and governance
- Represent AI program to board, regulators, stakeholders
- Champion responsible AI practices across organization

Model Risk Manager

Purpose: Lead second line of defense for model risk

Responsibilities:
- Develop and maintain model governance policies and procedures
- Chair Model Risk Committee
- Oversee model risk assessments and tiering
- Coordinate model validation activities
- Maintain model inventory and governance documentation
- Monitor model performance and compliance
- Escalate issues to AI Governance Committee
- Serve as governance subject matter expert

Model Owner (First Line)

Purpose: Business accountability for specific model(s)

Responsibilities:

Back to Document Index

- Business accountability for model performance and outcomes
- Approve model requirements and use cases
- Ensure model aligns with business objectives
- Provide resources for model development and maintenance
- Monitor business KPIs and model value realization
- Approve model changes and updates
- Participate in model validation and testing

Model Developer (First Line)

Purpose: Technical development and maintenance of models

Responsibilities:
- Design, develop, and test models per requirements
- Create comprehensive model documentation
- Conduct model testing and validation
- Implement model monitoring and alerting
- Perform model maintenance and updates
- Respond to model issues and incidents
- Comply with governance policies and standards

Model Validator (Second Line)

Purpose: Independent validation of models

Responsibilities:
- Conduct independent model validation per governance policy
- Assess model methodology, data, implementation, and performance
- Test model accuracy, robustness, and limitations
- Evaluate bias, fairness, and ethical considerations
- Document validation findings and recommendations
- Track remediation of validation findings
- Provide validation approval/rejection recommendation

Compliance & Legal

Purpose: Ensure models comply with laws, regulations, policies

Responsibilities:
- Assess regulatory compliance (AI Act, GDPR, industry regulations)
- Review model documentation for compliance adequacy
- Identify legal and regulatory risks
- Provide guidance on emerging regulations
- Support regulatory examinations and audits
- Review model use cases for ethical and legal issues

Back to Document Index

4. Model Lifecycle Governance

Models progress through defined lifecycle stages from conception through retirement. Each stage has specific activities, deliverables, and governance gates (approval checkpoints) to ensure appropriate oversight and control.

Stage 1: Ideation & Business Case

Purpose: Evaluate business opportunity and determine if AI/ML is appropriate solution

Key Activities:
• Define business problem and success criteria
• Assess feasibility of AI/ML approach
• Conduct preliminary risk assessment
• Develop business case with ROI analysis
• Identify data requirements and availability
• Determine initial risk tier

Key Deliverables:
• AI Opportunity Assessment (Template 1.1)
• Preliminary Risk Assessment
• Business Case with ROI projections

Governance Gate: Model Risk Committee approval to proceed to development

Gate Criteria:
• Clear business value and measurable success criteria
• AI/ML is appropriate solution vs. alternatives
• Acceptable preliminary risk profile
• Data availability sufficient for model development
• Resources allocated and committed

Stage 2: Development & Training

Purpose: Build, train, and test model to meet requirements

Key Activities:
• Collect and prepare training data
• Develop model architecture and algorithms
• Train and tune model
• Conduct development testing (accuracy, bias, robustness)
• Create model documentation
• Perform comprehensive risk assessment

Back to Document Index

Key Deliverables:
• Trained model artifacts
• Model Development Documentation (methodology, data, assumptions, limitations)
• Testing Results (accuracy, performance, bias testing)
• AI Risk Assessment Report (Template 6.1)
• Model Risk Tier determination

Governance Gate: Independent model validation

Gate Criteria:
• Model meets accuracy and performance requirements
• Comprehensive documentation completed
• Testing demonstrates acceptable bias and fairness
• Risk assessment completed and reviewed
• Model ready for independent validation

Stage 3: Validation

Purpose: Independent review and challenge of model by second line of defense

Key Activities:
• Independent assessment of model methodology
• Validation of model data quality and appropriateness
• Testing of model accuracy and performance
• Bias and fairness assessment
• Review of model limitations and assumptions
• Assessment of implementation and controls
• Evaluation of model documentation adequacy

Key Deliverables:
• Model Validation Report
• Findings and Recommendations
• Validation Approval/Rejection decision

Governance Gate: Deployment approval based on risk tier
• Low Risk: Model Risk Committee
• Medium Risk: Model Risk Committee
• High Risk: AI Governance Committee
• Critical Risk: AI Governance Committee + Board notification

Gate Criteria:
• Satisfactory validation findings (or acceptable remediation plan)
• All critical and high findings addressed
• Model documentation complete and adequate

Back to Document Index

• Monitoring and controls in place
• Risk acceptance documented and approved

Stage 4: Deployment

Purpose: Move model into production environment with appropriate controls

Key Activities:
• Deploy model to production infrastructure
• Implement monitoring and alerting
• Configure performance dashboards
• Conduct user training
• Execute communication plan
• Activate support processes
• Perform post-deployment validation

Key Deliverables:
• Deployed production model
• Monitoring dashboards and alerts
• Operational runbooks
• Training materials and documentation
• Post-deployment validation results

Governance Gate: Production readiness review

Gate Criteria:
• Successful deployment to production
• Monitoring and alerts operational
• Support processes activated
• User training completed
• Post-deployment testing successful
• Rollback procedures tested and ready

Stage 5: Monitoring & Operation

Purpose: Ongoing model operation with continuous monitoring and maintenance

Key Activities:
• Monitor model performance metrics
• Track data drift and model drift
• Review bias and fairness metrics
• Conduct periodic model validation
• Manage model incidents and issues
• Perform routine maintenance and updates
• Generate periodic performance reports

Back to Document Index

Key Deliverables:
• Model Performance Dashboard (ongoing)
• Quarterly Performance Reports
• Annual Model Validation
• Incident Reports (as needed)

Governance Gate: Periodic reviews based on risk tier
• Critical/High Risk: Quarterly review by Model Risk Committee
• Medium Risk: Semi-annual review by Model Risk Committee
• Low Risk: Annual review

Gate Criteria:
• Performance within acceptable thresholds
• No significant drift or degradation
• Bias metrics within tolerance
• All incidents resolved
• Periodic validation satisfactory

Stage 6: Change Management

Purpose: Govern changes to model, data, or environment

Key Activities:
• Assess change impact and risk
• Update model documentation
• Test changes in non-production
• Conduct targeted validation
• Obtain approval based on change significance
• Deploy changes with appropriate controls

Key Deliverables:
• Change Request Documentation
• Change Impact Assessment
• Testing Results
• Updated Model Documentation

Governance Gate: Change approval based on significance
• Material Changes: Full validation + governance committee approval
• Moderate Changes: Targeted validation + Model Risk Committee approval
• Minor Changes: Testing + Model Owner approval

Gate Criteria:
• Change justified with clear business rationale
• Impact assessed and documented

Back to Document Index

• Testing completed successfully
• Documentation updated
• Rollback plan prepared

Stage 7: Retirement

Purpose: Decommission model when no longer needed or replaced

Key Activities:
• Develop retirement plan
• Communicate to stakeholders
• Transition users to alternative
• Archive model artifacts and documentation
• Decommission infrastructure
• Conduct lessons learned review

Key Deliverables:
• Model Retirement Plan
• Archived Documentation and Artifacts
• Lessons Learned Report
• Decommissioning Confirmation

Governance Gate: Retirement approval

Gate Criteria:
• Retirement justified (replaced, obsolete, or no longer needed)
• Stakeholders notified and impacted users transitioned
• Documentation and artifacts archived per retention policy
• Infrastructure decommissioned
• Lessons learned captured

Back to Document Index

5. Model Risk Tiering System

Not all models carry equal risk. The model risk tiering system classifies models into risk categories (Critical, High, Medium, Low) to apply proportionate governance—more oversight and controls for higher-risk models, streamlined processes for lower-risk models. This ensures efficient use of governance resources while maintaining appropriate risk management.

Risk Tier Determination Criteria

Assess models across multiple dimensions to determine risk tier:

Business Impact:

- Critical: Strategic decisions, significant financial impact (>$10M), core business processes
- High: Important decisions, material financial impact ($1-10M), key business processes
- Medium: Tactical decisions, moderate financial impact ($100K-1M), supporting processes
- Low: Minor decisions, minimal financial impact (<$100K), optional enhancements

Decision Autonomy:

- Critical: Fully automated decisions affecting individuals (hiring, credit, healthcare)
- High: Automated decisions with limited human review
- Medium: Recommendations to humans who make final decisions
- Low: Insights or analytics supporting human analysis

Regulatory Scrutiny:

- Critical: Regulated use cases (credit decisioning, medical diagnosis, employment)
- High: Emerging regulatory attention (AI Act high-risk systems)
- Medium: General data protection regulations (GDPR, CCPA)
- Low: Minimal regulatory implications

Potential for Harm:

- Critical: Could cause severe harm to individuals or protected groups
- High: Could cause significant individual or reputational harm
- Medium: Could cause moderate inconvenience or concern
- Low: Minimal potential for harm

Data Sensitivity:

- Critical: Highly sensitive personal data (health, biometric, financial)
- High: Personal identifiable information (PII), confidential business data

Back to Document Index

• Medium: Limited personal data, internal business data
• Low: Public or anonymized data

Model Complexity:

• Critical: Black-box deep learning, limited explainability
• High: Complex ensemble models, moderate explainability
• Medium: Standard ML algorithms (random forest, gradient boosting)
• Low: Simple models (linear regression, decision trees)

Reputational Risk:

• Critical: Public-facing, high visibility, brand critical
• High: Customer-facing, moderate visibility
• Medium: Internal use, limited external visibility
• Low: Back-office, no external visibility

Risk Tier Governance Requirements

Each risk tier has specific governance requirements:

CRITICAL RISK TIER

Approval Authority: AI Governance Committee + Board notification

Validation Requirements:
• Full independent validation by senior model validators
• External validation or audit (recommended)
• Bias and fairness assessment by ethics expert
• Legal and compliance review

Documentation Requirements:
• Comprehensive model documentation (all components)
• Model card for stakeholder transparency
• Algorithmic Impact Assessment
• Compliance documentation for all applicable regulations

Monitoring Requirements:
• Real-time performance monitoring
• Daily automated alerts
• Weekly performance reports
• Quarterly governance review
• Annual comprehensive validation

Change Management:

Back to Document Index

• All changes require full validation
• AI Governance Committee approval for material changes
• Regression testing on all changes

HIGH RISK TIER

Approval Authority: AI Governance Committee

Validation Requirements:
• Full independent validation
• Bias and fairness assessment
• Compliance review

Documentation Requirements:
• Comprehensive model documentation
• Model card recommended
• Risk assessment and mitigation plan

Monitoring Requirements:
• Automated performance monitoring
• Weekly automated alerts
• Monthly performance reports
• Quarterly governance review
• Annual validation

Change Management:
• Material changes require full validation
• Model Risk Committee approval
• Testing on all changes

MEDIUM RISK TIER

Approval Authority: Model Risk Committee

Validation Requirements:
• Targeted independent validation
• Basic bias assessment

Documentation Requirements:
• Standard model documentation
• Risk assessment

Monitoring Requirements:
• Automated performance monitoring
• Monthly performance reports
• Semi-annual governance review

Back to Document Index

• Bi-annual validation

Change Management:
• Material changes require targeted validation
• Model Risk Committee approval for significant changes
• Testing on significant changes

LOW RISK TIER

Approval Authority: Model Owner + Model Risk Manager notification

Validation Requirements:
• Self-validation with peer review
• Documentation review by Model Risk Manager

Documentation Requirements:
• Basic model documentation
• Simple risk assessment

Monitoring Requirements:
• Basic performance monitoring
• Quarterly performance reports
• Annual review

Change Management:
• Model Owner approval
• Testing on material changes
• Notification to Model Risk Manager

Risk Tier Examples

Critical Risk Examples:

• AI model approving/denying credit applications
• AI assisting in medical diagnosis or treatment recommendations
• AI making hiring or promotion decisions
• AI determining insurance premiums or coverage
• AI used in criminal justice (recidivism prediction, sentencing)
• AI controlling autonomous vehicles or safety-critical systems

High Risk Examples:

• AI recommending products or content with significant purchase impact
• AI detecting fraud with automatic account suspension
• AI screening job applications (with human final decision)
• AI pricing products dynamically

Back to Document Index

- AI determining customer service priority
- AI optimizing supply chain with significant cost impact

Medium Risk Examples:

- AI categorizing customer support tickets
- AI recommending upsells or cross-sells
- AI forecasting inventory needs
- AI routing work assignments
- AI generating marketing content
- AI analyzing survey responses

Low Risk Examples:

- AI suggesting meeting times
- AI organizing email inbox
- AI creating data visualizations
- AI spell-checking and grammar suggestions
- AI recommending training courses
- AI analyzing public social media trends

Back to Document Index

6. Model Inventory and Documentation Requirements

Comprehensive model inventory and documentation enables effective governance, risk management, and compliance. Organizations must maintain current, accurate records of all AI/ML models in development and production.

Model Inventory

Maintain centralized model inventory containing:

- Model ID (unique identifier)
- Model Name and Business Purpose
- Model Owner and Model Developer
- Model Type/Algorithm (e.g., neural network, random forest, LLM)
- Risk Tier (Critical/High/Medium/Low)
- Lifecycle Stage (Development, Validation, Production, Retired)
- Deployment Date and Last Update Date
- Business Unit and Use Case
- Data Sources and Features Used
- Performance Metrics and Thresholds
- Validation Status and Next Validation Date
- Regulatory Classification (e.g., EU AI Act risk level)
- Dependencies (upstream data, downstream systems)
- Documentation Location (links to detailed docs)
- Contact Information (owner, developer, validator)

The model inventory should be maintained in an accessible system (database, governance platform) with version control and audit trail. Review and update monthly at minimum.

Model Documentation Requirements

Required documentation varies by risk tier:

Model Development Documentation (All Tiers)

• Business Objective: Problem being solved, success criteria
• Model Methodology: Algorithm choice, architecture, training approach
• Data: Sources, preparation, features, quality assessment
• Assumptions and Limitations: Known constraints, edge cases
• Performance Metrics: Accuracy, precision, recall, AUC, or relevant metrics
• Testing Results: Development testing, bias testing, robustness testing
• Version History: Changes over time

Back to Document Index

Model Validation Documentation (Medium/High/Critical)

- Validation Approach: Methodology, scope, independence
- Validation Findings: Strengths, weaknesses, issues identified
- Recommendations: Required improvements, risk mitigations
- Validation Conclusion: Approval/rejection, conditions
- Validator Information: Who conducted validation, qualifications

Model Risk Assessment (All Tiers)

- Risk Identification: Potential risks across all categories
- Risk Analysis: Likelihood and impact assessment
- Risk Mitigation: Controls and monitoring to address risks
- Residual Risk: Remaining risk after mitigation
- Risk Tier Determination: Rationale for tier assignment

Model Card (High/Critical)

Stakeholder-facing summary containing:

- Model Purpose: What does it do?
- Intended Use Cases: What is it designed for?
- Out-of-Scope Uses: What should it NOT be used for?
- Training Data: What data was used? Any limitations?
- Performance Metrics: How accurate is it? Any performance differences across groups?
- Limitations: What are its constraints and weaknesses?
- Ethical Considerations: Fairness, bias, potential harms
- Contact Information: Who to contact with questions

Operational Documentation (All Tiers)

- Deployment Guide: How to deploy and configure
- Monitoring Guide: Metrics to track, alert thresholds
- Incident Response: How to handle errors or issues
- Maintenance Procedures: Routine updates and care
- User Guide: How to use model outputs
- Rollback Procedures: How to revert if needed

Compliance Documentation (High/Critical)

- Regulatory Assessment: Which regulations apply?
- Compliance Requirements: Specific requirements to meet
- Compliance Evidence: How requirements are satisfied
- Algorithmic Impact Assessment: For high-risk systems
- Data Privacy Assessment: DPIA if processing personal data
- Audit Trail: Records demonstrating compliance

Back to Document Index

7. Model Monitoring and Performance Management

Continuous monitoring ensures models perform as expected, identifies degradation early, and enables proactive intervention before issues impact business or stakeholders.

Key Monitoring Dimensions

Model Performance Monitoring

Track core metrics:
• Accuracy, Precision, Recall, F1 Score (classification)
• RMSE, MAE, R-squared (regression)
• Business metrics (conversion rate, revenue impact, error rate)

Set thresholds:
• Performance floor (minimum acceptable performance)
• Alert threshold (degradation requiring investigation)
• Critical threshold (degradation requiring immediate action)

Monitoring frequency:
• Critical/High: Daily automated monitoring
• Medium: Weekly monitoring
• Low: Monthly monitoring

Data Drift Monitoring

Detect changes in input data distribution:
• Statistical tests (KS test, chi-square test)
• Distribution comparison over time
• Feature distribution shifts
• Missing value rates

Actions when drift detected:
• Investigate root cause
• Assess impact on model performance
• Determine if retraining needed
• Update model or adjust data pipeline

Model Drift Monitoring (Concept Drift)

Detect when relationship between inputs and outputs changes:
• Prediction distribution changes
• Performance degradation over time
• Actual outcomes vs. predictions divergence

Actions when model drift detected:

Back to Document Index

• Trigger model retraining
• Update model with recent data
• Re-validate model performance
• Obtain approval for updated model

Bias and Fairness Monitoring

Track fairness metrics across demographic groups:
• Performance parity (equal accuracy across groups)
• Demographic parity (equal positive prediction rates)
• Equal opportunity (equal true positive rates)
• Predictive parity (equal precision across groups)

Compare performance:
• Across protected characteristics (race, gender, age)
• Over time (is bias changing?)
• Against fairness thresholds

Actions when bias detected:
• Investigate root cause in data or algorithm
• Implement bias mitigation techniques
• Consider fairness-aware algorithms
• Escalate to governance committee if severe

Operational Monitoring

Track system health:
• Prediction latency and throughput
• Error rates and failure modes
• System availability and uptime
• Resource utilization (compute, memory)

Business monitoring:
• Usage patterns and volume
• User adoption and satisfaction
• Business value realization
• Cost per prediction

Monitoring Dashboard Requirements

Create monitoring dashboards showing:

- Current performance vs. baseline and thresholds (visual indicators)
- Performance trends over time (line charts showing degradation)
- Data drift indicators (distribution comparisons)
- Bias and fairness metrics by protected group
- Alert status (active alerts, recent alerts, alert history)

Back to Document Index

- Model metadata (version, last updated, risk tier)
- Recent predictions and outcomes (sample monitoring)
- Links to detailed documentation and runbooks

Alert and Escalation Procedures

Define tiered alert and escalation process:

Level 1 - Informational Alert:
Minor threshold breach, no immediate action required. Email to model owner and developer. Investigate within 5 business days.

Level 2 - Warning Alert:
Performance degradation or drift detected. Immediate notification to model owner, developer, and Model Risk Manager. Investigate within 24 hours. Create an incident ticket.

Level 3 - Critical Alert:
Severe performance degradation, bias spike, or system failure. Immediate notification to model owner, developer, Model Risk Manager, and Model Owner's director. Convene incident response team. Assess the need for immediate model shutdown. Escalate to the AI Governance Committee within 24 hours.

Back to Document Index

8. Model Change Management

Models require updates over time due to data drift, new requirements, or performance improvements. Robust change management ensures changes are controlled, tested, and approved appropriately.

Change Classification

Classify changes by significance to determine governance requirements:

Material Changes (High Impact)

Definition: Significant changes affecting model behavior, performance, or risk profile

Examples:
- Algorithm change (e.g., switching from random forest to neural network)
- Major feature additions or removals
- Training data source changes
- Significant performance impact (>5% accuracy change)
- New use cases or populations
- Changes affecting regulatory compliance

Governance Requirements:
- Full documentation update
- Complete validation (same rigor as initial validation)
- AI Governance Committee approval (Critical/High risk models)
- Model Risk Committee approval (Medium risk models)
- Comprehensive testing including bias and fairness
- Risk re-assessment

Moderate Changes (Medium Impact)

Definition: Changes with moderate impact on model behavior

Examples:
- Model retraining with same methodology but updated data
- Hyperparameter tuning
- Minor feature engineering changes
- Performance improvements (2-5% accuracy change)
- Infrastructure or deployment changes

Governance Requirements:
- Documentation update for changed components
- Targeted validation (focused on changed areas)

Back to Document Index

- Model Risk Committee approval (Critical/High risk)
- Model Owner approval (Medium/Low risk)
- Testing focused on changes
- Performance comparison pre/post change

Minor Changes (Low Impact)

Definition: Small changes with minimal impact

Examples:
- Bug fixes
- Documentation updates
- UI/dashboard changes
- Monitoring improvements
- Performance <2% change

Governance Requirements:
- Document change in change log
- Model Owner approval
- Basic testing
- Notification to Model Risk Manager

Change Management Process

Follow structured process for all model changes:

1. Change Request: Document proposed change, rationale, expected impact

2. Change Classification: Determine if Material, Moderate, or Minor

3. Impact Assessment: Analyze impact on performance, risk, compliance, stakeholders

4. Testing Plan: Define testing approach appropriate to change significance

5. Development & Testing: Implement change in non-production, conduct testing

6. Validation: Conduct validation appropriate to change classification

7. Approval: Obtain required approval based on change classification and risk tier

8. Deployment: Deploy to production with appropriate controls

9. Monitoring: Enhanced monitoring post-change to detect issues early

10. Documentation: Update all affected documentation and model inventory

Back to Document Index

9. Model Retirement

Models should be retired when they are no longer needed, have been replaced by better alternatives, or can no longer meet performance or compliance requirements. Structured retirement ensures smooth transitions.

Reasons for Model Retirement

- • Model replaced by improved version or alternative approach
- • Business use case no longer exists or has changed significantly
- • Model performance degraded beyond acceptable levels and cannot be salvaged
- • Regulatory changes make model non-compliant and remediation infeasible
- • Cost of maintenance exceeds value delivered
- • Technology obsolescence (e.g., legacy platform being sunset)
- • Strategic decision to discontinue AI for this use case
- • Risk profile has changed making model unacceptable

Model Retirement Process

1. Retirement Proposal

Document:
• Reason for retirement
• Impact on stakeholders and business processes
• Alternative approach (replacement model, manual process, discontinue capability)
• Timeline and transition plan

2. Stakeholder Communication

Notify:
• Model users and affected business units
• Downstream systems dependent on model outputs
• IT operations and infrastructure teams
• Governance committees

Provide adequate notice period (typically 30-90 days depending on criticality)

3. Transition Execution

• Deploy replacement model or alternative process
• Train users on new approach
• Run parallel operations during transition (if feasible)
• Monitor for issues during transition

4. Decommissioning

• Disable model endpoints and APIs
• Remove production access

Back to Document Index

• Decommission infrastructure
• Archive monitoring dashboards

5. Documentation and Archival

Archive per retention policy:
• Model artifacts and code
• Training data (if retention required)
• Documentation (development, validation, operational)
• Performance history and monitoring data
• Incident history
• Retirement rationale and lessons learned

Typical retention: 5-7 years for regulatory purposes

6. Lessons Learned

Conduct retrospective:
• What worked well?
• What challenges were encountered?
• How could the model have been improved?
• What should future models learn from this experience?
• Were there governance or oversight gaps?

Share findings to improve future models

7. Formal Closure

• Update model inventory to "Retired" status
• Document retirement completion
• Obtain sign-off from Model Owner and Model Risk Manager
• Close any open incidents or change requests

Back to Document Index

10. Best Practices for Model Governance

1. Start with Risk-Based Approach

Not all models need the same level of governance. Apply proportionate oversight based on risk tier. Avoid over-governing low-risk models (wastes resources) or under-governing high-risk models (creates exposure). Regularly reassess risk tiers as models, use cases, or environments change.

2. Embed Governance Early

Integrate governance into model development from the start, not as afterthought before deployment. Early governance prevents costly rework, ensures proper documentation, and builds quality in rather than inspecting it in. Shift-left on validation, testing, and documentation.

3. Make Governance Enabling, Not Blocking

Position governance as enabler of responsible innovation, not bureaucratic obstacle. Streamline processes, provide templates and tools, offer guidance rather than just rules. Well-designed governance accelerates deployment by preventing issues, not delaying it.

4. Maintain Independence in Validation

Model validation must be truly independent—validators should not report to model developers, should not have built the model, and should have authority to reject models. Independence ensures objective assessment and credible challenge. Avoid conflicts of interest.

5. Automate Where Possible

Automate monitoring, testing, documentation generation, compliance checks. Manual processes do not scale as the model portfolio grows. Automation ensures consistency, reduces human error, and frees the governance team for high-value judgment tasks. Use governance platforms and MLOps tools.

6. Document Everything

If it is not documented, it did not happen. Comprehensive documentation is essential for governance, compliance, auditability, knowledge transfer, and incident response. Invest in documentation templates, standards, and tools. Make documentation part of "definition of done."

7. Monitor Continuously

Model governance does not end at deployment. Continuous monitoring detects degradation, drift, bias, and issues. Set up automated monitoring with clear thresholds and escalation. Review monitoring data regularly. Treat monitoring as an operational requirement, not optional.

Back to Document Index

8. Foster Collaboration Across Lines of Defense

First line (developers), second line (governance), and third line (audit) should collaborate, not operate in silos. Regular communication, shared tools, and mutual respect prevent adversarial relationships. Governance is a team sport.

9. Invest in Governance Capability

Model governance requires skilled people, appropriate tools, and adequate time. Underfunded governance creates risk. Hire or develop model validators, invest in governance platforms, allocate dedicated governance resources. Governance is not free but is cheaper than failures.

10. Learn from Incidents

When model issues occur, conduct thorough retrospectives. Identify root causes, update governance policies and processes, share lessons across organizations. Incidents are learning opportunities. Maintain an incident database to track patterns.

11. Stay Current with Regulations

AI regulations are evolving rapidly (EU AI Act, US executive orders, industry standards). Monitor regulatory developments, assess impact on governance framework, adapt proactively. Engage legal/compliance early. Better to lead than react.

12. Communicate Governance Value

Articulate how governance reduces risk, enables innovation, builds trust, supports compliance. Share success stories (issues prevented, faster deployments through good process). Make governance visible and valued, not hidden compliance tax.

Back to Document Index

11. Common Pitfalls to Avoid

1. One-Size-Fits-All Governance

Applying the same governance to all models regardless of risk. Low-risk models get over-governed (wasted effort), high-risk models get under-governed (unacceptable risk). Solution: Implement risk-based tiering with proportionate controls.

2. Governance as Afterthought

Treating governance as the final gate before deployment rather than integrated into development. Results in rushed validation, incomplete documentation, and deployment delays. Solution: Embed governance throughout lifecycle from ideation.

3. Validation Lacking Independence

Model developers validating their own work or validators reporting to development managers. Creates conflicts of interest, reduced objectivity, insufficient challenge. Solution: Ensure true independence through a separate reporting structure.

4. Documentation Debt

Postponing documentation until later, resulting in incomplete, inaccurate, or missing documentation. Future teams cannot maintain models, audits fail, compliance issues arise. Solution: Documentation is mandatory deliverable at each stage.

5. Set and Forget Monitoring

Setting up monitoring dashboards but not actively reviewing or responding to alerts. Degradation goes unnoticed until major issues occur. Solution: Assign monitoring ownership, establish review cadence, enforce response SLAs.

6. Governance Theater

Creating governance processes that look impressive but lack substance—checking boxes without rigor. Models approved without real validation, policies without enforcement. Solution: Focus on effectiveness over appearances. Measure outcomes.

7. Ignoring Model Drift

Failing to retrain or update models as data and relationships change over time. The model becomes stale, performance degrades, but continues operating. Solution: Proactive drift monitoring and scheduled retraining or refresh.

8. Unclear Accountability

No one clearly owns model outcomes, governance process, or incident response. Issues fall through cracks. Solution: Explicit ownership documented in inventory. RACI matrix for governance activities.

Back to Document Index

9. Over-Reliance on Tools

Believing governance platforms or MLOps tools solve governance challenges. Tools enable governance but do not replace policies, processes, or human judgment. Solution: Implement framework first, then select tools to support it.

10. Insufficient Governance Capacity

Too few governance staff for too many models. Validators overwhelmed, reviews rushed, backlogs grow. Solution: Scale governance capacity with model portfolio. Automate where possible.

11. No Escalation Path

When issues arise, there is no clear path to raise concerns or get decisions. Problems linger unresolved. Solution: Define escalation procedures, empower governance teams, ensure executive accessibility.

12. Compliance-Only Mindset

Viewing governance solely as a regulatory compliance burden rather than risk management and value enabler. A minimalist approach creates vulnerabilities. Solution: Position governance as enabler of responsible, trustworthy AI.

Back to Document Index

12. Appendices

Appendix A: Sample Governance Committee Charter

AI GOVERNANCE COMMITTEE CHARTER

Purpose:
Provide strategic oversight and governance of the organization's AI/ML program to ensure responsible, ethical, compliant, and value-creating deployment of artificial intelligence.

Authority:
• Approve AI governance framework, policies, and standards
• Approve deployment of Critical and High risk models
• Establish risk appetite and tolerance for AI initiatives
• Allocate resources for AI governance and risk management
• Escalate material AI risks to Board of Directors
• Resolve disputes and exceptions to governance policies

Membership:
• Chair: Chief Data/Analytics Officer (or equivalent AI leader)
• Chief Technology Officer
• Chief Information Officer
• Chief Risk Officer
• General Counsel or Chief Legal Officer
• Chief Compliance Officer
• Business Unit Leaders (as appropriate)
• Model Risk Manager (non-voting, secretariat)

Meeting Cadence: Quarterly at minimum, monthly during high-activity periods

Quorum: 60% of voting members, including Chair or delegate

Decision-Making: Consensus preferred; majority vote if consensus cannot be reached

Reporting: Provide quarterly reports to Board Audit Committee or Board Risk Committee

Appendix B: Sample Model Approval Form

MODEL APPROVAL REQUEST

Model Information:
Model ID: _____
Model Name: _____
Model Owner: _____
Model Developer: _____

Back to Document Index

Risk Tier: ☐ Critical ☐ High ☐ Medium ☐ Low

Business Case:
Business Problem: _____
Expected Value: _____
Success Metrics: _____

Model Details:
Algorithm Type: _____
Training Data: _____
Performance Metrics: _____

Risk Assessment:
Key Risks Identified: _____
Mitigation Strategies: _____
Residual Risks: _____

Validation Results:
Validator Name: _____
Validation Date: _____
Validation Conclusion: ☐ Approved ☐ Approved with Conditions ☐ Rejected
Key Findings: _____

Compliance:
☐ GDPR/Privacy requirements assessed
☐ Regulatory requirements reviewed
☐ Bias and fairness tested
☐ Documentation complete

Approvals:
Model Owner: _____ Date: _____
Model Validator: _____ Date: _____
Model Risk Manager: _____ Date: _____
Committee Chair (if required): _____ Date: _____

Appendix C: Professional Standards Alignment

This Model Governance Framework aligns with industry standards and best practices for AI/ML governance:

BABOK (Business Analysis Body of Knowledge) Alignment:

Back to Document Index

• Requirements Life Cycle Management (3.1): Managing model requirements through lifecycle
• Solution Evaluation (6): Evaluating model performance and value
• Business Analysis Governance (3.5): Establishing governance for analysis work
• Change Strategy (7.2): Managing organizational change for AI adoption

PMBOK (Project Management Body of Knowledge) Alignment:

• Integration Management (4): Coordinating all aspects of model governance
• Scope Management (5): Defining and controlling model scope
• Risk Management (11): Comprehensive model risk management
• Quality Management (8): Ensuring model quality and performance
• Stakeholder Management (13): Managing model stakeholders

DMBOK (Data Management Body of Knowledge) Alignment:

• Data Governance (3): Governing data used in models
• Data Quality Management (13): Ensuring quality of model data
• Metadata Management (12): Documenting model metadata
• Data Security (7): Protecting sensitive model data
• Data Architecture (4): Designing data flows for models

AI/ML Governance Frameworks and Standards:

This framework incorporates principles from:

• NIST AI Risk Management Framework (AI RMF): Comprehensive risk management approach for AI systems
• ISO/IEC 42001:2023 AI Management System: International standard for AI management
• ISO/IEC 23894:2023 AI Risk Management: Guidance on AI risk management
• Model Risk Management (SR 11-7): US Federal Reserve guidance on model risk management
• EU AI Act: Risk-based regulatory framework for AI systems
• OECD AI Principles: Responsible stewardship of trustworthy AI
• IEEE 7000 Series: Standards for ethical AI design and governance
• Partnership on AI: Best practices for responsible AI development

Financial Services Model Risk Management:

For organizations in financial services, this framework aligns with:
• SR 11-7 (Supervisory Guidance on Model Risk Management): Federal Reserve model risk guidance
• OCC Bulletin 2011-12: Model validation guidance

Back to Document Index

• ECB Guide on Model Risk Management: European Central Bank guidance
• Basel Committee Principles for Model Risk Management

Healthcare AI Governance:

For healthcare AI applications:
• FDA Software as Medical Device (SaMD): Regulatory framework for AI/ML medical devices
• Good Machine Learning Practice (GMLP): Principles for healthcare AI
• HIPAA Security and Privacy Rules: Protecting patient data in AI systems
• WHO Ethics and Governance of AI for Health

Back to Document Index

Document Usage Rights and Disclaimer

This Business Analysis Template for AI Projects is provided as a starter document to assist business analysts in assessing organizational readiness for AI adoption.

Usage Rights:

✓ You may freely use, modify, and customize this template for your projects

✓ You may adapt the readiness assessment framework to fit your needs

✓ You may incorporate this into your organizational assessment processes

✓ You may share this template within your organization

Restrictions:

✗ You may not resell, redistribute, or commercialize this template

✗ You may not claim original authorship of this framework

✗ You may not remove these usage rights statements

Disclaimer:

This template is provided as-is without warranties. While it incorporates professional best practices for readiness assessment and organizational change management, users are responsible for adapting methods to their specific context. The template should be customized based on your unique needs and validated with appropriate subject matter experts including change management professionals, organizational development specialists, and business leaders. Readiness assessment requires understanding of both technical capabilities and organizational dynamics.