Back to Document Index

AI Risk Assessment Report

Business Analysis Template for AI Projects

Template ID:	6.1
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) Feasibility & ROI Analysis (1.4)

1. Document Purpose

This AI Risk Assessment Report provides a comprehensive framework for systematically identifying, analyzing, and mitigating risks specific to AI initiatives. Effective risk management is critical for AI projects due to their unique technical, ethical, regulatory, and operational challenges that differ from traditional IT implementations.

Key purposes of this document include:

- Identify comprehensive range of AI-specific risks across technical, operational, and business domains
- Assess likelihood and impact of each risk using structured methodology
- Prioritize risks based on potential severity and organizational risk appetite
- Develop specific mitigation strategies and controls for high-priority risks
- Establish monitoring and escalation mechanisms for ongoing risk management
- Support informed decision-making about AI project feasibility and approach
- Ensure compliance with regulatory requirements and industry standards
- Provide transparency for governance boards, executives, and stakeholders
- Create audit trail demonstrating due diligence in risk management
- Enable continuous risk assessment throughout AI project lifecycle

2. When to Use This Template

Use this template at key decision points and milestones throughout the AI project lifecycle. Risk assessment should be iterative, not one-time, as risks evolve with project progress.

Back to Document Index

Ideal Use Cases:

Project Initiation: Before committing resources, assess whether risks are acceptable and manageable given organizational risk appetite.

Business Case Development: Include comprehensive risk assessment in feasibility analysis to inform go/no-go decisions.

Architecture and Design: Evaluate technical risks associated with proposed AI solution architecture and approach.

Vendor Selection: Assess risks specific to third-party AI models, platforms, or services being considered.

Pre-Deployment Review: Comprehensive risk validation before production launch to ensure mitigations are effective.

Regulatory Submissions: Demonstrate risk management due diligence for compliance with AI regulations and industry standards.

Quarterly Reviews: Ongoing monitoring to identify new risks or changes in existing risk profiles.

Incident Response: After AI-related incidents, update risk assessment and strengthen controls.

Scope Changes: When adding capabilities or expanding to new use cases, assess incremental risks.

Audit Preparation: Provide evidence of systematic risk identification and mitigation for internal or external audits.

3. How to Use This Template (Risk Assessment Process)

Follow this systematic process to conduct comprehensive AI risk assessments. Effective risk management requires structured identification, analysis, mitigation planning, and ongoing monitoring.

Step 1: Define Assessment Scope

Clarify what is being assessed: specific AI model, entire initiative, particular use case, or deployment environment. Define boundaries clearly. Include stakeholders, systems, data, and processes in scope. Identify key assumptions. Document assessment timeframe and review frequency. Clear scope prevents gaps and ensures comprehensive coverage.

Back to Document Index

Step 2: Assemble Risk Assessment Team

Include diverse perspectives: data scientists (technical risks), legal/compliance (regulatory risks), security (cybersecurity risks), business leaders (strategic risks), ethics/DEI (fairness/bias risks), operations (deployment risks). Multi-disciplinary teams identify risks that homogeneous groups miss. Assign risk assessment owner and document participants.

Step 3: Identify Risks Systematically

Use multiple approaches: review risk catalogs and taxonomies, conduct brainstorming sessions, analyze similar AI projects, review incident databases, consult subject matter experts, assess regulatory requirements, evaluate vendor risks. Document each risk with clear description, potential causes, and consequences. Cast wide net—can prioritize later.

Step 4: Analyze and Assess Each Risk

For each identified risk, evaluate:

- Likelihood: What is the probability of occurrence? (Rare, Unlikely, Possible, Likely, Almost Certain)
- Impact: What are consequences if realized? (Negligible, Minor, Moderate, Major, Severe)
- Velocity: How quickly could impact occur? (Slow, Medium, Fast)
- Detection: How easily can we detect occurrences? (Easy, Moderate, Difficult)

Use consistent scales and criteria. Document rationale for ratings. Consider both immediate and long-term impacts.

Step 5: Calculate Risk Level

Combine likelihood and impact to determine overall risk level:

- Critical Risk (Red): Immediate action required, may be project-stopping
- High Risk (Orange): Urgent attention needed, escalate to leadership
- Medium Risk (Yellow): Manage with defined controls and monitoring
- Low Risk (Green): Accept with basic monitoring

Use risk matrix (likelihood × impact) for consistent prioritization. Consider organizational risk appetite when setting thresholds.

Step 6: Develop Mitigation Strategies

For each significant risk, define response strategy:

- Avoid: Change approach to eliminate risk (different technology, narrower scope)
- Mitigate: Reduce likelihood or impact through controls and safeguards
- Transfer: Shift risk to third party (insurance, vendor contracts, partnerships)
- Accept: Acknowledge risk and proceed with monitoring

Document specific actions, owners, timelines, and success criteria. Ensure mitigations are feasible and resourced.

Back to Document Index

Step 7: Define Controls and Monitoring

Establish preventive controls (stop risks from occurring) and detective controls (identify when they occur). Define monitoring metrics and thresholds. Create escalation procedures for risk materialization. Assign control owners. Document testing and validation approach. Build monitoring into operational processes, not separate activity.

Step 8: Document Residual Risk

After mitigation strategies, reassess:

- Residual Likelihood: What is probability after controls?
- Residual Impact: What are consequences if it still occurs?
- Residual Risk Level: Is remaining risk acceptable?

Be realistic—no mitigation eliminates risk entirely. Document explicitly what risk remains and why it is acceptable. Escalate if residual risk exceeds organizational tolerance.

Step 9: Create Risk Register

Consolidate all findings in a structured risk register. For each risk: ID number, description, category, likelihood, impact, risk level, mitigation strategy, owner, timeline, status, residual risk. Maintain a living document. Update as the project progresses and new information emerges.

See: 6_1_AI_Risk_Register_SAMPLE.xlsx

Step 10: Communicate and Obtain Approval

Present risk assessment to decision-makers: governance boards, executives, steering committees. Provide executive summary highlighting critical and high risks. Explain mitigation approach and required resources. Obtain formal approval to proceed or decision to pause/stop. Document approvals and risk acceptance in project records.

Back to Document Index

4. AI-Specific Risk Categories

AI initiatives face unique risks beyond traditional IT projects. Use this comprehensive taxonomy to ensure thorough risk identification across all critical domains.

Model Performance and Accuracy Risks

Risks related to AI models functioning below expectations or making incorrect predictions/decisions.

Specific Risks:
• Insufficient Accuracy: Model fails to meet minimum accuracy thresholds for production use
• Performance Degradation: Model accuracy declines over time as data patterns shift (model drift)
• Edge Cases and Outliers: Model fails on rare but important scenarios not well-represented in training data
• False Positives/Negatives: Unacceptable rates of incorrect classifications with business consequences
• Overfitting: Model performs well on training data but poorly on new, real-world data
• Generalization Failure: Model does not transfer well across different contexts or populations

Potential Impacts:
• Incorrect business decisions based on faulty predictions
• Customer dissatisfaction from poor service quality
• Financial losses from process errors
• Regulatory sanctions if performance falls below required standards

Key Mitigations:
• Establish minimum performance thresholds before deployment
• Implement continuous model monitoring and retraining
• Maintain human oversight for high-stakes decisions
• Build robust testing with diverse, representative datasets
• Create fallback procedures for when model confidence is low

Data Quality and Availability Risks

Risks associated with data used for training, validation, and production inference.

Specific Risks:
• Insufficient Training Data: Not enough data to train robust, accurate models
• Poor Data Quality: Inaccurate, incomplete, inconsistent, or outdated data compromises model

Back to Document Index

• Unrepresentative Data: Training data does not reflect production environment or population diversity
• Data Drift: Statistical properties of production data change over time, degrading model performance
• Data Pipeline Failures: Systems feeding data to model fail, causing delays or errors
• Missing Features: Critical variables unavailable in production that were present in training
• Label Quality Issues: Incorrect or inconsistent labels in training data introduce errors

Potential Impacts:
• Models that do not generalize or perform poorly in production
• Delayed go-live while collecting additional data
• Ongoing maintenance burden addressing data quality issues
• System downtime when data pipelines fail

Key Mitigations:
• Conduct comprehensive data quality assessment early
• Establish data quality standards and validation processes
• Implement data monitoring and alerting
• Build redundancy into data pipelines
• Create data labeling quality control processes
• Plan for data drift detection and model retraining

Bias, Fairness, and Discrimination Risks

Risks that AI perpetuates or amplifies unfair outcomes across demographic groups.

Specific Risks:
• Historical Bias: Training data reflects past discriminatory practices that model learns and perpetuates
• Representation Bias: Underrepresentation of certain groups leads to poorer performance for those groups
• Measurement Bias: Features or labels systematically disadvantage certain populations
• Algorithmic Bias: Model architecture or learning process amplifies existing biases
• Deployment Bias: Model used in ways that create discriminatory outcomes even if model itself is fair
• Intersectional Bias: Compound disadvantage at intersections of multiple characteristics

Potential Impacts:
• Legal liability under anti-discrimination laws and regulations
• Reputational damage and loss of customer trust
• Regulatory sanctions and fines
• Ethical violations and harm to affected individuals
• Employee morale issues if internal AI systems are biased

Back to Document Index

Key Mitigations:
• Conduct fairness assessment using appropriate metrics for context
• Test model performance across demographic groups
• Implement bias testing in model development and validation
• Use fairness-aware algorithms and techniques
• Establish diverse review teams for fairness assessment
• Create monitoring and auditing processes for ongoing fairness
• Maintain human oversight for high-stakes decisions affecting individuals

Explainability and Transparency Risks

Risks from inability to explain how AI makes decisions or what factors influence outcomes.

Specific Risks:
• Black Box Models: Complex models (deep learning) difficult or impossible to explain
• Lack of Decision Transparency: Inability to show which factors drove specific decisions
• Regulatory Non-Compliance: Failure to meet explainability requirements (e.g., GDPR right to explanation)
• Stakeholder Distrust: Users, customers, or regulators do not trust opaque systems
• Audit Challenges: Difficulty demonstrating compliance or investigating incidents
• Debugging Difficulty: Hard to diagnose and fix errors without understanding model logic

Potential Impacts:
• Regulatory penalties for insufficient transparency
• Customer complaints and loss of trust
• Difficulty obtaining stakeholder buy-in for deployment
• Extended debugging time when issues arise
• Legal challenges when decisions affect individuals

Key Mitigations:
• Evaluate explainability requirements early in model selection
• Use interpretable models when possible (decision trees, linear models)
• Implement explainability techniques (SHAP, LIME) for complex models
• Document decision logic and key factors influencing predictions
• Create audit trails showing model inputs and outputs
• Provide user-friendly explanations for affected stakeholders

Security and Adversarial Risks

Risks from malicious attacks targeting AI systems or data.

Specific Risks:
• Adversarial Attacks: Carefully crafted inputs designed to fool model into incorrect predictions
• Data Poisoning: Malicious actors inject bad data into training set to compromise model
• Model Theft: Proprietary models stolen through APIs or reverse engineering

Back to Document Index

• Privacy Attacks: Model inadvertently reveals sensitive information about training data (model inversion)
• Denial of Service: Attacks that overwhelm AI system or prevent legitimate use
• Prompt Injection: For LLMs, malicious prompts that bypass safety controls

Potential Impacts:
• Compromised model integrity and incorrect decisions
• Intellectual property theft
• Privacy breaches exposing sensitive data
• System downtime and business disruption
• Loss of competitive advantage if proprietary models are stolen

Key Mitigations:
• Implement adversarial testing and robustness evaluation
• Secure training data and pipelines with access controls
• Use techniques like differential privacy to prevent information leakage
• Monitor for anomalous inputs or usage patterns
• Implement rate limiting and input validation
• Conduct regular security assessments and penetration testing
• Protect model artifacts with encryption and access controls

Data Privacy and Confidentiality Risks

Risks of unauthorized access, use, or disclosure of sensitive personal or business data.

Specific Risks:
• Personal Data Exposure: AI systems process or reveal personally identifiable information (PII) inappropriately
• Re-identification: Anonymized data in training sets can be re-identified through model outputs
• Data Retention Violations: Keeping data longer than permitted by policy or regulation
• Cross-Border Data Transfer: Moving data across jurisdictions in violation of data localization laws
• Unauthorized Access: Insufficient access controls allow improper data access
• Data Minimization Failure: Collecting or using more personal data than necessary
• Consent Violations: Using data without proper consent or for purposes beyond consent scope

Potential Impacts:
• Regulatory fines (GDPR, CCPA, HIPAA violations)
• Privacy breach notifications and remediation costs
• Reputational damage and customer churn
• Legal liability and class action lawsuits
• Loss of customer trust

Back to Document Index

Key Mitigations:
• Conduct Privacy Impact Assessment (PIA) or Data Protection Impact Assessment (DPIA)
• Implement privacy-by-design principles
• Use techniques like federated learning, differential privacy, or homomorphic encryption
• Establish data minimization practices
• Implement robust access controls and encryption
• Document consent and data usage purposes clearly
• Create data retention and deletion policies

Regulatory and Compliance Risks

Risks of violating laws, regulations, or industry standards governing AI use.

Specific Risks:
• Regulatory Non-Compliance: Failure to meet emerging AI regulations (EU AI Act, sector-specific rules)
• Lack of Documentation: Insufficient records to demonstrate compliance with regulatory requirements
• Prohibited Use Cases: Deploying AI for applications banned or restricted by regulation
• Audit Failure: Unable to provide evidence of compliance during regulatory audits
• Changing Requirements: Regulations evolve faster than compliance can be maintained
• Industry Standards: Non-compliance with relevant standards (ISO, NIST AI frameworks)
• Cross-Jurisdictional Conflicts: Different requirements across regions where AI operates

Potential Impacts:
• Regulatory fines and penalties
• Forced suspension or shutdown of AI systems
• Increased regulatory scrutiny and oversight
• Reputational damage
• Delayed deployment while achieving compliance

Key Mitigations:
• Conduct regulatory landscape analysis for all relevant jurisdictions
• Maintain regulatory compliance matrix and monitoring process
• Implement governance framework aligned with regulations
• Create comprehensive documentation (model cards, impact assessments, audit trails)
• Engage legal/compliance teams early and throughout project
• Build compliance requirements into development and testing
• Establish ongoing regulatory monitoring and adaptation process

Operational and Integration Risks

Risks related to deploying and operating AI in production environments.

Specific Risks:

Back to Document Index

• Deployment Failures: Technical issues preventing successful production deployment
• Integration Complexity: Difficulty integrating AI with existing systems and processes
• Scalability Issues: AI cannot handle production volumes or performance requirements
• Infrastructure Failures: Insufficient compute, storage, or network resources
• Dependency Risks: Reliance on third-party services, APIs, or models that may change or fail
• Maintenance Burden: Ongoing operational costs exceed expectations or capacity
• Technical Debt: Shortcuts taken during development create long-term maintenance issues
• Skills Gap: Insufficient internal expertise to operate and maintain AI systems

Potential Impacts:
• Failed deployment or extended delays
• System downtime and business disruption
• Poor user experience from performance issues
• Higher-than-planned operational costs
• Inability to maintain or enhance system over time

Key Mitigations:
• Conduct comprehensive technical feasibility assessment
• Prototype and test integration early
• Perform load testing and scalability validation
• Build monitoring and observability into architecture
• Create operational runbooks and procedures
• Develop skills through training or hiring
• Establish vendor management and contingency plans
• Plan for technical debt management and system evolution

Business and Strategic Risks

Risks affecting business value, ROI, and strategic objectives.

Specific Risks:
• ROI Shortfall: Benefits do not materialize or costs exceed projections
• Adoption Failure: Stakeholders do not use AI system as expected
• Change Resistance: Organizational resistance prevents effective deployment
• Competitive Risk: Competitors implement superior AI capabilities first
• Vendor Lock-In: Dependence on single vendor limits flexibility and increases costs
• Opportunity Cost: Resources invested in AI unavailable for other priorities
• Scope Creep: Expanding requirements increase costs and delay delivery
• Misaligned Incentives: AI optimizes for wrong metrics or creates unintended consequences

Potential Impacts:
• Failed business case and wasted investment

Back to Document Index

• Loss of competitive advantage
• Organizational disruption without commensurate benefits
• Damage to AI program credibility affecting future initiatives
• Strategic misalignment and resource misallocation

Key Mitigations:
• Develop robust business case with realistic assumptions
• Implement strong change management and adoption programs
• Pilot with small scope before full deployment
• Monitor actual benefits realization against projections
• Design for vendor portability where feasible
• Establish governance to manage scope and priorities
• Align AI metrics with strategic objectives
• Build stakeholder engagement from project start

Reputational and Ethical Risks

Risks to organizational reputation and ethical standing from AI use.

Specific Risks:
• Public Backlash: Negative media coverage or social media reaction to AI use
• Customer Distrust: Loss of customer confidence from perceived AI misuse
• Employee Concerns: Internal opposition if AI is seen as threatening jobs or unethical
• Ethical Violations: AI used in ways inconsistent with organizational values
• Transparency Failures: Lack of openness about AI use erodes trust
• Unintended Consequences: AI creates harmful outcomes not anticipated
• Stakeholder Harm: AI disadvantages or harms individuals or communities

Potential Impacts:
• Brand damage and loss of customer loyalty
• Boycotts or activist campaigns
• Difficulty attracting and retaining talent
• Loss of social license to operate
• Regulatory attention triggered by public pressure
• Shareholder concern affecting valuation

Key Mitigations:
• Establish AI ethics principles and governance
• Conduct ethical impact assessments
• Create transparency in AI use and capabilities
• Implement stakeholder engagement and communication plans
• Build human oversight for sensitive decisions
• Establish clear accountability for AI outcomes

Back to Document Index

- Monitor for unintended consequences and respond quickly
- Create mechanisms for stakeholder concerns and redress

Back to Document Index

5. Risk Rating Scales and Assessment Matrix

See: 6_1_Risk_Rating_Matrix.xlsx

Use consistent, well-defined scales to ensure objective, comparable risk ratings across all assessments.

Likelihood Scale (Probability of Occurrence)

1 - Rare: May occur only in exceptional circumstances (< 10% probability)

2 - Unlikely: Could occur but not expected (10-30% probability)

3 - Possible: Might occur at some point (30-50% probability)

4 - Likely: Will probably occur (50-75% probability)

5 - Almost Certain: Expected to occur in most circumstances (> 75% probability)

Impact Scale (Consequences if Risk Occurs)

1 - Negligible: Minimal impact on project or operations. Easily managed with existing resources. No regulatory, financial, or reputational consequences.

2 - Minor: Limited impact requiring some attention. Minor delays or cost increases (< 5%). Minimal stakeholder concern. No lasting consequences.

3 - Moderate: Noticeable impact requiring management attention. Delays of 1-3 months or cost increases of 5-15%. Some stakeholder concerns. Manageable regulatory/compliance issues.

4 - Major: Significant impact threatening project success. Major delays (3-6 months) or cost overruns (15-30%). Serious regulatory issues. Potential reputational damage. Executive escalation required.

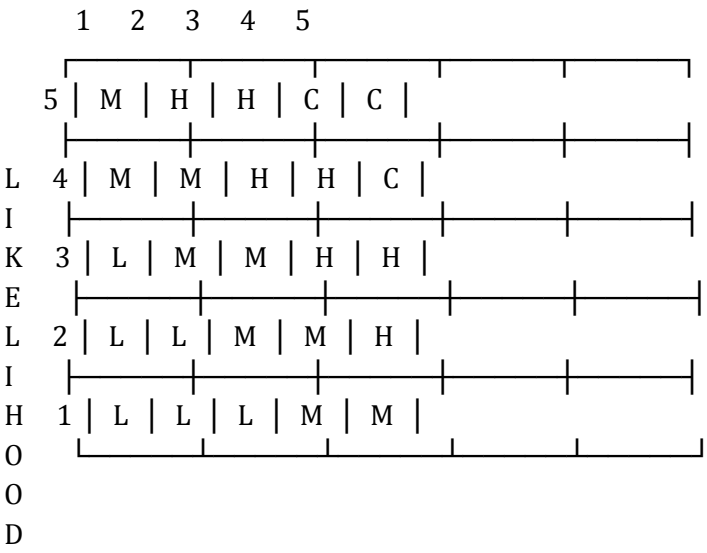
5 - Severe: Critical impact potentially causing project failure. Delays > 6 months or cost overruns > 30%. Severe regulatory penalties. Significant reputational damage. May require project cancellation.

Risk Level Matrix (Likelihood × Impact)

Combine likelihood and impact to determine overall risk level:

IMPACT

Back to Document Index



Legend:
L = Low Risk (Green) - Accept with basic monitoring
M = Medium Risk (Yellow) - Manage with defined controls
H = High Risk (Orange) - Urgent attention and mitigation required
C = Critical Risk (Red) - Immediate action required, may block deployment

Risk Response Strategies by Risk Level

Critical Risk (Red): Immediate escalation to executive leadership. Develop a comprehensive mitigation plan before proceeding. May require project pause or cancellation if unmitigatable. Weekly monitoring required.

High Risk (Orange): Escalate to project sponsor and governance board. Mandatory mitigation plan with specific actions, owners, and timelines. Bi-weekly monitoring required. Cannot deploy without residual risk acceptance.

Medium Risk (Yellow): Active management by project team. Define controls and monitoring approach. Monthly review of status. Document in risk register with mitigation plans.

Low Risk (Green): Accept with basic awareness and periodic monitoring. Document in risk register. Review quarterly or if circumstances change.

Back to Document Index

6. Best Practices for AI Risk Assessment

1. Start Early and Iterate

Conduct initial risk assessment during project conception, not before deployment. Risk profile changes as project progresses—reassess at major milestones. Early identification enables proactive mitigation rather than reactive crisis management.

2. Involve Diverse Perspectives

Homogeneous teams miss risks. Include technical experts, business leaders, legal/compliance, ethics, security, and affected stakeholders. Different backgrounds identify different risks. Diversity reduces blind spots.

3. Be Comprehensive but Prioritize

Cast a wide net during identification—do not self-censor. Document all identified risks. Then prioritize ruthlessly based on likelihood and impact. Focus mitigation efforts on critical and high risks. Monitor medium and low risks but do not over-invest.

4. Use Data and Evidence

Support risk ratings with data: incident history, industry benchmarks, research findings, pilot results. Avoid purely subjective assessments. Evidence-based ratings are more defensible and lead to better decisions.

5. Document Thoroughly

Risk assessments serve multiple purposes: decision-making, compliance, audits, lessons learned. Document risk descriptions, likelihood/impact rationale, mitigation strategies, ownership, and decisions. In the future you will thank the current you.

6. Make Risks Actionable

Vague risks lead to vague mitigations. "AI might not work" is not actionable. "Model accuracy may fall below the 85% threshold due to insufficient training data" enables specific action. Be specific about causes, consequences, and potential mitigations.

7. Link to Governance

Risk assessment should inform governance decisions: go/no-go, resource allocation, scope changes, deployment timing. Establish clear escalation paths. Define risk acceptance authority levels. Connect risk management to decision-making processes.

8. Monitor Continuously

Risk assessment is not one-time. Risks evolve as the project progresses, external environment changes, or new information emerges. Build ongoing monitoring into project rhythms. Update risk register regularly. Re-assess at milestones.

Back to Document Index

9. Plan for Residual Risk

No mitigation eliminates risk completely. Be explicit about what risk remains after mitigation. Ensure residual risk is acceptable to the organization. Document who accepted residual risk and when. Create response plans for if residual risks materialize.

10. Learn from Experience

Track which risks materialized and effectiveness of mitigations. Conduct retrospectives after incidents. Update risk catalogs based on lessons learned. Share risk insights across AI projects to elevate organizational maturity.

11. Balance Risk and Innovation

The goal is not zero risk—that prevents innovation. The goal is informed risk-taking where benefits justify risks. Some AI initiatives will fail—that is expected. Focus on managing risks to acceptable levels while enabling valuable innovation.

12. Communicate Transparently

Hiding or minimizing risks does not make them disappear. Transparent communication builds trust. Stakeholders and leadership can handle bad news better than surprises. Present risks honestly alongside mitigation plans and residual risk.

Back to Document Index

7. Common Pitfalls to Avoid

1. Assessing Too Late

Conducting risk assessment right before deployment when the project is already committed and mitigation options are limited. Result: Either deploy with known unacceptable risks or delay while scrambling to mitigate. Solution: Assess early and often.

2. Technical Focus Only

Focusing exclusively on technical/model risks while ignoring compliance, ethical, reputational, or business risks. AI projects fail more often from non-technical risks. Solution: Use comprehensive risk taxonomy covering all domains.

3. Optimism Bias

Underestimating likelihood or impact because the team is excited about AI or confident in capabilities. Wishful thinking is not risk management. Solution: Use evidence and data. Seek outside perspectives. Document rationale for ratings.

4. Analysis Paralysis

Getting stuck in endless risk analysis without making decisions or taking action. Trying to identify every possible risk. Solution: Set time limits. Focus on material risks. Recognizing perfection is impossible. Make decisions with available information.

5. Generic Mitigations

Listing generic, non-specific mitigations like "implement controls" or "monitor performance" without concrete actions, owners, or timelines. Solution: Define specific, actionable mitigations with clear ownership, resources, and success criteria.

6. No Clear Ownership

Identifying risks but not assigning clear owners for monitoring and mitigation. Unowned risks do not get managed. Solution: Every significant risk needs a named owner accountable for managing it.

7. Ignoring Regulatory Landscape

Failing to consider emerging AI regulations and compliance requirements. AI regulation is evolving rapidly. Yesterday's acceptable practice may be tomorrow's violation. Solution: Engage legal/compliance early. Monitor regulatory developments actively.

8. Assuming Mitigations Work

Implementing mitigations but not validating effectiveness. Controls may not work as intended. Solution: Test mitigations. Monitor for actual risk reduction. Adjust if mitigations prove ineffective.

Back to Document Index

9. Siloed Assessment

Each team conducts their own risk assessment in isolation. Results in gaps, inconsistencies, and failure to connect risks. Solution: Coordinate assessments across teams. Use consistent methodology and scales. Share findings.

10. Poor Documentation

Conducting assessment but not documenting findings, rationale, or decisions adequately. When auditors, regulators, or future teams ask, no one remembers. Solution: Document as you go. Create an audit trail. Maintain a risk register as a living document.

11. Treating as Compliance Exercise

Completing risk assessment to check box rather than genuinely managing risks. Going through motions without changing behavior. Solution: Use risk assessment to inform real decisions. Link to governance and resource allocation. Make it meaningful.

12. No Follow-Through

Creating comprehensive risk registers and mitigation plans that sit in the drawer while the project proceeds unchanged. Solution: Build risk management into project processes. Track mitigation completion. Hold owners accountable. Review risks in governance meetings.

Back to Document Index

8. Appendices

Appendix A: Sample Risk Register (AI Document Processing)

See: 6_1_AI_Risk_Register_SAMPLE.xlsx

Example risk register showing comprehensive AI risk assessment

Risk ID | Risk Description | Category | L | I | Risk Level | Mitigation Strategy | Owner | Residual

---

R-001 | Model accuracy falls below 95% threshold making automated processing unreliable | Model Performance | 3 | 4 | HIGH | Extend training data to 500K+ documents. Implement confidence thresholds with human review for <95% confidence cases. | Data Science Lead | MEDIUM

R-002 | Training data reflects historical biases leading to differential treatment of vendors | Bias/Fairness | 4 | 5 | CRITICAL | Conduct fairness assessment across vendor types. Implement a fairness-aware algorithm. Test performance by vendor demographic. Create a bias monitoring dashboard. | Ethics Officer | MEDIUM

R-003 | Personal data in invoices exposed through model or logging | Data Privacy | 2 | 5 | HIGH | Implement data minimization. Remove PII before training. Use differential privacy techniques. Encrypt data at rest and in transit. Conduct DPIA. | Privacy Officer | LOW

R-004 | Unable to explain why specific invoice was rejected/approved | Explainability | 4 | 3 | HIGH | Implement SHAP explainability for complex cases. Create decision audit trails. Provide user-facing explanations. Document decision logic. | ML Engineer | MEDIUM

R-005 | GDPR compliance failure due to insufficient data governance | Regulatory | 2 | 5 | HIGH | Engage legal counsel for GDPR assessment. Implement data retention policies. Create consent management. Document processing purposes. Enable data subject rights. | Compliance Lead | LOW

R-006 | Users reject AI system due to poor change management | Business/Adoption | 3 | 4 | HIGH | Develop a comprehensive change management plan. Conduct training. Address job security concerns. Implement pilot with champions. Build feedback loops. | Change Manager | MEDIUM

Back to Document Index

R-007 | Model performance degrades over time as invoice formats evolve | Model Drift | 4 | 3 | HIGH | Implement continuous monitoring for accuracy drift. Create automated alerts at <97% accuracy. Plan quarterly model retraining. Monitor data distribution shifts. | MLOps Lead | MEDIUM

R-008 | Integration with ERP system fails causing data loss or corruption | Operational | 2 | 4 | MEDIUM | Conduct integration testing early. Implement transaction rollback. Create data validation. Build monitoring and alerts. Develop rollback procedures. | Integration Lead | LOW

Legend:

L = Likelihood (1-5), I = Impact (1-5)

Risk Level: CRITICAL (Red) | HIGH (Orange) | MEDIUM (Yellow) | LOW (Green)

Appendix B: Risk Assessment Worksheet Template

Use this template to document each identified risk systematically

RISK ASSESSMENT WORKSHEET

Risk ID:

_____

Risk Title:

_____

Risk Category:

☐ Model Performance ☐ Data Quality ☐ Bias/Fairness ☐ Explainability
☐ Security ☐ Privacy ☐ Regulatory ☐ Operational ☐ Business ☐ Reputational

Risk Description:

Describe the risk clearly and specifically:

Back to Document Index

Potential Causes:

What could cause this risk to occur?

Potential Consequences:

What happens if this risk occurs?

INHERENT RISK ASSESSMENT (Before Mitigation):

Likelihood (1-5):

___ Rationale:

Impact (1-5):

___ Rationale:

Risk Level:

☐ Critical ☐ High ☐ Medium ☐ Low

MITIGATION STRATEGY:

Response Strategy:

☐ Avoid ☐ Mitigate ☐ Transfer ☐ Accept

Specific Mitigation Actions:

1.
2.
3.

Back to Document Index

Mitigation Owner:

_____ Target Date: _____

Resources Required:

Success Criteria:

How will we know mitigation is effective?

RESIDUAL RISK ASSESSMENT (After Mitigation):

Residual Likelihood (1-5):

___ Residual Impact (1-5): ___

Residual Risk Level:

☐ Critical ☐ High ☐ Medium ☐ Low

Is Residual Risk Acceptable?

☐ Yes ☐ No

If No, Additional Actions:

Risk Accepted By:

_____ Date: _____

Review Frequency:

☐ Weekly ☐ Bi-weekly ☐ Monthly ☐ Quarterly

Last Reviewed:

_____ Status: ☐ Open ☐ Mitigated ☐ Closed

Back to Document Index

Appendix C: Risk Monitoring Dashboard Template

Track risk status and mitigation progress at a glance

See: 6_1_Risk_Rating_Matrix.xlsx

RISK DASHBOARD - [Project Name] - [Date]

Risk Summary by Level:

- Critical Risks: ___ (Red)
- High Risks: ___ (Orange)
- Medium Risks: ___ (Yellow)
- Low Risks: ___ (Green)
- Total Risks: ___

Risk Trend (vs. Last Review):

- New Risks Identified: ___
- Risks Escalated: ___
- Risks Reduced: ___
- Risks Closed: ___

Top 5 Risks Requiring Attention:

- 1. [Risk ID - Risk Title - Owner - Status]
- 2. [Risk ID - Risk Title - Owner - Status]
- 3. [Risk ID - Risk Title - Owner - Status]
- 4. [Risk ID - Risk Title - Owner - Status]
- 5. [Risk ID - Risk Title - Owner - Status]

Mitigation Actions Status:

- Completed: ___
- On Track: ___
- At Risk: ___
- Overdue: ___

Recent Risk Events:

Back to Document Index

- [Date]: [Description of risk that materialized and response]
- [Date]: [Description of risk that materialized and response]

Escalations Required:

☐ [Risk requiring executive decision]
☐ [Risk requiring resource allocation]
☐ [Risk requiring scope/timeline change]

Appendix D: Risk Assessment Checklist

Use this checklist to ensure comprehensive risk assessment

Preparation:

☐ Assessment scope clearly defined
☐ Multi-disciplinary team assembled
☐ Risk assessment methodology selected
☐ Relevant documentation reviewed (architecture, business case, feasibility)
☐ Similar project risks and incidents researched
☐ Stakeholder interviews scheduled

Risk Identification:

☐ Model performance and accuracy risks identified
☐ Data quality and availability risks identified
☐ Bias, fairness, and discrimination risks identified
☐ Explainability and transparency risks identified
☐ Security and adversarial risks identified
☐ Data privacy and confidentiality risks identified
☐ Regulatory and compliance risks identified
☐ Operational and integration risks identified
☐ Business and strategic risks identified
☐ Reputational and ethical risks identified

Risk Analysis:

☐ Likelihood assessed for each risk (1-5 scale)
☐ Impact assessed for each risk (1-5 scale)

Back to Document Index

☐ Risk level calculated (likelihood × impact)
☐ Velocity and detection difficulty considered
☐ Ratings supported with evidence and rationale
☐ Risks prioritized using consistent criteria

Mitigation Planning:

☐ Response strategy selected for each significant risk
☐ Specific mitigation actions defined
☐ Mitigation owners assigned
☐ Implementation timelines established
☐ Success criteria defined
☐ Resource requirements identified
☐ Dependencies and constraints documented

Controls and Monitoring:

☐ Preventive controls defined
☐ Detective controls defined
☐ Monitoring metrics and thresholds established
☐ Escalation procedures created
☐ Review frequency determined
☐ Control owners assigned

Residual Risk:

☐ Residual likelihood and impact assessed
☐ Residual risk level acceptable to organization
☐ Risk acceptance documented with approvals
☐ Contingency plans created for high residual risks

Documentation:

☐ Risk register created and populated
☐ Individual risk assessments documented
☐ Rationale for ratings captured
☐ Mitigation plans detailed
☐ Approvals and decisions recorded
☐ Assessment methodology documented

Back to Document Index

Communication and Approval:

☐ Risk assessment report prepared
☐ Executive summary created
☐ Findings presented to governance board
☐ Critical and high risks escalated
☐ Stakeholder questions addressed
☐ Formal approval obtained to proceed

Appendix E: Professional Standards Alignment

This template aligns with industry-standard frameworks and best practices for AI risk management:

BABOK (Business Analysis Body of Knowledge) Alignment:

• Risk Analysis and Management (10.3): Systematic identification and assessment of risks
• Requirements Risk Analysis (3.5.4): Assessing risks to requirements realization
• Solution Evaluation (6): Evaluating solution risks and performance
• Business Analysis Planning and Monitoring (3): Incorporating risk management into planning

PMBOK (Project Management Body of Knowledge) Alignment:

• Project Risk Management (11): Comprehensive risk management processes
• Plan Risk Management (11.1): Defining risk management approach
• Identify Risks (11.2): Systematic risk identification
• Perform Qualitative Risk Analysis (11.3): Assessing likelihood and impact
• Plan Risk Responses (11.4): Developing mitigation strategies
• Monitor Risks (11.6): Tracking and updating risk status

DMBOK (Data Management Body of Knowledge) Alignment:

• Data Governance (3): Governing data risks in AI systems
• Data Security (7): Protecting data from unauthorized access and use
• Data Quality Management (13): Managing data quality risks
• Data Privacy and Protection: Ensuring privacy and compliance

AI-Specific Risk Frameworks Alignment:

Back to Document Index

This template incorporates principles and practices from:
• NIST AI Risk Management Framework (NIST AI RMF): Comprehensive AI risk management approach
• ISO/IEC 23894:2023: Information technology - Artificial intelligence - Risk management
• EU AI Act: Risk classification and requirements for high-risk AI systems
• IEEE 7010-2020: Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems
• OECD AI Principles: Risk-based approach to trustworthy AI
• ISO/IEC 42001: AI Management System standard

Regulatory Compliance Frameworks:

Risk assessment supports compliance with:
• GDPR (General Data Protection Regulation): Data Protection Impact Assessments (DPIAs)
• CCPA/CPRA (California Consumer Privacy Act): Privacy risk assessments
• HIPAA (Health Insurance Portability and Accountability Act): Security risk analysis
• SOC 2 (Service Organization Control): Risk assessment for service organizations
• Industry-specific regulations: Financial services, healthcare, government

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.