# NC-AI-001: AI Risk Register Template

## Document Information

**Standard**: Northern Cascadia AI Governance Standard NC-AI-001  
**Title**: AI Risk Register Template  
**Version**: 1.0  
**Publication Date**: Q1 2026  
**Publisher**: Kaizen Strategic AI (Northern Cascadia Institute of AI Governance)  
**Based On**: ISO 42001:2023 (AI Management Systems)  
**License**: Public Domain - Free for use and adaptation

## Purpose

This template provides a comprehensive, ISO 42001-compliant framework for identifying, assessing, and managing AI-related risks in your organization. Use this template to:

1. Systematically identify AI risks across your operations
2. Assess impact and likelihood using standard risk matrices
3. Document controls and mitigation strategies
4. Track risk treatment progress
5. Maintain compliance with ISO 42001 requirements

**Who should use this**: Any organization implementing AI systems, from small businesses to large enterprises, particularly those pursuing ISO 42001 certification.

**How to use**: Fill out one risk register per AI system or per organizational scope. This template includes pre-populated risk categories based on ISO 42001 requirements, ISO 23894 (AI risk management), and real-world implementation insights.

## Instructions for Use

### Step 1: Define Your Scope

Before filling out the template, clearly define: - Which AI system(s) are you assessing? - What is the intended use of the AI system? - Who are the stakeholders affected? - What is your organization’s role? (Developer / Provider / User / Multiple)

### Step 2: Identify Risks

Review each risk category below and identify which risks apply to your AI system. For each risk: - Describe the specific risk scenario - Assess Impact (1-5 scale) - Assess Likelihood (1-5 scale) - Calculate Risk Score - Identify existing or planned controls

### Step 3: Implement Controls

For each risk identified: - Design appropriate controls - Assign ownership - Set target treatment dates - Track implementation progress

### Step 4: Regular Review

Review this register: - Monthly: Update status of in-progress controls - Quarterly: Re-assess risk scores based on controls implemented - Annually: Comprehensive review of all risks and controls - After incidents: Immediate reassessment triggered by any incident

## Risk Scoring Matrix

### Impact Scale (1-5)

| Score | Impact Level | Description | Examples |
| --- | --- | --- | --- |
| 5 | Catastrophic | Severe irreversible damage, business failure | Personal injury, company insolvency, major legal liability |
| 4 | Critical | Major damage requiring significant resources to recover | Major data breach, regulatory investigation, loss of major client |
| 3 | High | Significant impact requiring immediate attention | Operational disruption, reputation damage, compliance violation |
| 2 | Moderate | Noticeable impact that can be managed | Minor service disruption, customer complaints, minor financial loss |
| 1 | Low | Minimal impact, easily managed | Minimal operational effect, low-cost fixes |

### Likelihood Scale (1-5)

| Score | Likelihood | Description | Frequency |
| --- | --- | --- | --- |
| 5 | Almost Certain | Will occur in most circumstances | >80% probability within 12 months |
| 4 | Likely | Will probably occur in most circumstances | 50-80% probability within 12 months |
| 3 | Possible | Might occur at some time | 20-50% probability within 12 months |
| 2 | Unlikely | Could occur but not expected | 5-20% probability within 12 months |
| 1 | Rare | May occur only in exceptional circumstances | <5% probability within 12 months |

### Risk Score Calculation

**Risk Score = Impact × Likelihood**

Risk scores range from 1 to 25. Use the color-coded matrix below:

| Risk Score | Risk Level | Color | Action Required |
| --- | --- | --- | --- |
| 20-25 | Extreme | Red | Immediate action required, senior management involvement |
| 15-19 | High | Orange | Priority treatment within 30 days |
| 10-14 | Medium | Yellow | Treatment within 90 days |
| 5-9 | Low | Green | Monitor, treat as resources allow |
| 1-4 | Minimal | White | Accept, document decision |

### Risk Treatment Strategy

| Risk Level | Treatment Approach |
| --- | --- |
| **Extreme & High** | Mitigate - Must reduce to acceptable level |
| **Medium** | Mitigate or Accept - Decision based on cost/benefit |
| **Low & Minimal** | Accept or Treat - Document rationale |

## Risk Categories by ISO 42001

### Category 1: Bias and Fairness Risks

These risks relate to algorithmic bias, discrimination, and unfair outcomes.

#### 1.1 Algorithmic Bias in Decision-Making

**Risk Description**: AI system produces biased outputs that unfairly favor or disadvantage certain groups based on race, gender, age, or other protected characteristics.

**Examples**: - Hiring AI favoring male candidates over female candidates - Loan approval AI disproportionately denying applications from certain demographics - Healthcare AI providing different treatment recommendations based on protected attributes - Recruiting AI filtering out qualified candidates from underrepresented groups

**Potential Impacts**: - Legal liability and discrimination lawsuits - Regulatory investigations and penalties - Reputation damage and loss of trust - Loss of customers and business opportunities - Violation of human rights legislation

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] Not Started / [ ] In Progress / [ ] Complete |

#### 1.2 Unfair Treatment of Protected Groups

**Risk Description**: AI system fails to appropriately account for or accommodate protected groups, leading to exclusion or disadvantage.

**Examples**: - Facial recognition AI failing to accurately identify people with darker skin tones - Voice recognition AI struggling with non-native accents or speech patterns - Content recommendation AI reinforcing stereotypes about certain groups - AI screening tools excluding qualified candidates from marginalized communities

**Potential Impacts**: - Discrimination complaints and legal action - Regulatory non-compliance (human rights legislation) - Community backlash and media attention - Damage to brand and market position - Exclusion of valuable talent and perspectives

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 1.3 Lack of Representativeness in Training Data

**Risk Description**: Training data used to build the AI system is not representative of the target population, leading to biased model performance.

**Examples**: - Medical AI trained primarily on data from one demographic group - Language model trained on English-only content serving diverse multilingual users - Image recognition trained on Western faces serving global market - Product recommendation trained on data from one geographic region

**Potential Impacts**: - Model performs poorly for underrepresented groups - Compromised system effectiveness and user trust - Need for costly retraining and redeployment - Missed business opportunities in underserved markets - Regulatory scrutiny of data collection practices

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 1.4 Reinforcement of Harmful Stereotypes

**Risk Description**: AI system inadvertently perpetuates or amplifies negative stereotypes present in training data or society.

**Examples**: - Image generation AI producing stereotypical representations when prompted - Content moderation AI treating discussions of systemic bias as violations - Search ranking AI surfacing biased content preferentially - Advertisement targeting reinforcing demographic stereotypes

**Potential Impacts**: - Public criticism and social media backlash - Damage to brand reputation and customer relationships - Loss of partnership opportunities - Negative media coverage - Erosion of trust in AI capabilities

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

### Category 2: Security and Privacy Risks

These risks relate to data breaches, unauthorized access, and information security vulnerabilities.

#### 2.1 Unauthorized Access to AI Systems

**Risk Description**: Malicious actors gain unauthorized access to AI systems, models, or infrastructure.

**Examples**: - Hackers accessing cloud-based AI training environments - Insiders misusing elevated permissions to access sensitive AI models - Phishing attacks leading to credential theft for AI platforms - API keys exposed in public repositories

**Potential Impacts**: - Theft of proprietary models and training data - Service disruption or system shutdown - Financial losses from ransomware or business interruption - Regulatory fines for security breaches - Legal liability for data breach damages

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 2.2 Personal Information (PII) Data Breach

**Risk Description**: Personal information processed by or stored in AI systems is accessed, disclosed, or stolen without authorization.

**Examples**: - Customer data from AI chat logs exposed in data breach - Training data containing PII accidentally shared publicly - AI-generated insights revealing identifiable customer information - Third-party AI vendor experiencing data breach affecting your data

**Potential Impacts**: - PIPEDA/PIPA/privacy act compliance violations - Regulatory investigation and potential fines - Customer notification costs and remediation expenses - Class action lawsuits from affected individuals - Severe reputation damage and customer loss

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 2.3 Data Poisoning Attacks

**Risk Description**: Malicious actors intentionally corrupt training data to cause AI models to produce harmful outputs or fail.

**Examples**: - Adversarial actors injecting misleading data into public training datasets - Supply chain attacks compromising training data integrity - Model inversion attacks extracting sensitive information - Backdoor attacks embedding hidden triggers in model training

**Potential Impacts**: - Compromised model accuracy and reliability - Production system failures and service disruption - Security vulnerabilities allowing further exploitation - Need to retrain models from clean data - Loss of customer trust and business continuity

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 2.4 Model Theft and Intellectual Property Loss

**Risk Description**: Proprietary AI models, algorithms, or training data are stolen or reverse-engineered.

**Examples**: - Competitors using model extraction techniques to replicate functionality - Insiders selling proprietary model code to competitors - Cloud service provider breach exposing trained models - API endpoints allowing unlimited model querying for extraction

**Potential Impacts**: - Loss of competitive advantage and market position - Financial losses from stolen intellectual property - Erosion of unique value propositions - Damage to innovation investments - Difficulty enforcing IP rights

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 2.5 Inadequate Access Controls

**Risk Description**: Insufficient authentication, authorization, or access controls allow inappropriate access to AI systems or data.

**Examples**: - Shared credentials for multiple AI platform users - Overly permissive access granting users unnecessary privileges - Failed removal of access for terminated employees - Insufficient logging and monitoring of AI system access

**Potential Impacts**: - Unauthorized data access or model manipulation - Inability to detect security incidents or breaches - Compliance failures for access control requirements - Regulatory penalties for inadequate security - Legal liability for unauthorized access incidents

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

### Category 3: Transparency and Explainability Risks

These risks relate to the “black box” problem and lack of understanding of AI decision-making.

#### 3.1 Lack of Model Explainability

**Risk Description**: AI system produces decisions or outputs without clear explanation of reasoning, making it difficult to understand or challenge results.

**Examples**: - Deep learning model providing loan denial without explanation - AI hiring tool ranking candidates without transparency on criteria - Automated medical diagnosis without basis explanation - Fraud detection flagging transactions without cause disclosure

**Potential Impacts**: - Legal challenges to automated decisions - Regulatory non-compliance with right-to-explanation requirements - Loss of user trust and system adoption - Inability to debug or improve model performance - Audit and compliance failures

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 3.2 Black Box Decision-Making

**Risk Description**: Complex AI models operate in ways that are not understandable by humans, creating trust and compliance challenges.

**Examples**: - Neural networks with thousands of layers making critical decisions - Ensemble models combining multiple sub-models obscuring individual contributions - Reinforcement learning agents with evolving behaviors - Generative AI producing creative outputs with unknown reasoning

**Potential Impacts**: - Inability to validate or audit decision-making - Regulatory rejection of unexplained automated decisions - User rejection and low adoption rates - Ethical concerns about opaque decision-making - Risk of hidden biases or errors

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 3.3 Inadequate User Communication

**Risk Description**: Users are not properly informed about AI involvement in processes or how AI systems operate.

**Examples**: - Customers unaware AI is handling their support requests - Employees using AI tools without understanding limitations - Public interacting with AI-generated content believing it’s human-created - Stakeholders not informed about AI decision-making in critical processes

**Potential Impacts**: - Regulatory violation of disclosure requirements - Consumer protection lawsuits for deception - Loss of user trust when AI involvement discovered - Inappropriate reliance on AI without understanding - Ethical concerns about informed consent

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 3.4 Failure to Document AI Decision Logic

**Risk Description**: Organization fails to maintain adequate documentation of how AI systems make decisions, train models, or process data.

**Examples**: - No records of model training procedures or hyperparameters - Missing documentation of feature engineering decisions - Unclear documentation of decision thresholds or rules - Lost version control history for model iterations

**Potential Impacts**: - Inability to reproduce or audit AI decision-making - Compliance failures for documentation requirements - Difficulty debugging or improving systems - Legal challenges without supporting documentation - Regulatory scrutiny and penalties

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

### Category 4: Data Quality and Integrity Risks

These risks relate to poor quality, incomplete, or inappropriate training and operational data.

#### 4.1 Poor Training Data Quality

**Risk Description**: Training data used to develop AI models is incomplete, inaccurate, outdated, or inappropriate for the intended use.

**Examples**: - Training data with high percentage of duplicate or corrupted records - Outdated data not reflecting current market conditions or behaviors - Incomplete data with missing values improperly handled - Sourced data from inappropriate or irrelevant contexts

**Potential Impacts**: - Poor model performance and unreliable outputs - Failure to meet business objectives - Wasted development resources - Need for costly retraining - Production system failures

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 4.2 Incomplete Data Coverage

**Risk Description**: Training data does not adequately cover relevant scenarios, edge cases, or user populations.

**Examples**: - Training on normal operating conditions but not failure modes - Missing data for rare but critical events - Geographic bias with insufficient coverage for target markets - Temporal gaps in training data missing seasonal patterns

**Potential Impacts**: - Model failure in real-world edge cases - Poor performance for underrepresented scenarios - Inability to handle critical but rare events - User dissatisfaction and service disruptions - Safety or reliability failures

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 4.3 Data Integrity and Provenance Issues

**Risk Description**: Insufficient tracking of data lineage, source, transformations, or handling creates audit and quality challenges.

**Examples**: - Unable to trace data back to original sources - Unclear documentation of data transformations - Missing metadata about data collection methods - Unknown ownership or licensing of training data

**Potential Impacts**: - Compliance failures for data lineage requirements - Legal liability for unauthorized data use - Inability to audit data quality or sources - IP infringement risks - Regulatory investigation

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 4.4 Model Drift from Real-World Data

**Risk Description**: AI model performance degrades over time as real-world data distributions shift from training data.

**Examples**: - Consumer behavior changing after model deployment - Seasonal variations not accounted for in training data - Market conditions shifting due to external factors - Operational environments changing in unexpected ways

**Potential Impacts**: - Gradual decline in system accuracy and reliability - Silent failures going undetected - Business metrics deterioration - Customer dissatisfaction and churn - Need for expensive model retraining

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

### Category 5: Regulatory Compliance Risks

These risks relate to AI regulations, legal requirements, and compliance obligations.

#### 5.1 Non-Compliance with AI Regulations

**Risk Description**: Organization fails to comply with AI-specific regulations, standards, or legal requirements.

**Examples**: - Failure to conduct required impact assessments under EU AI Act - Not registering high-risk AI systems with regulatory authorities - Non-compliance with sector-specific AI regulations - Violation of emerging AI governance laws in various jurisdictions

**Potential Impacts**: - Regulatory investigations and enforcement actions - Financial penalties and sanctions - Mandatory system shutdowns - Legal liability and lawsuits - Market access restrictions

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 5.2 Insufficient Documentation for Compliance

**Risk Description**: Required documentation, assessments, or evidence for regulatory compliance is missing, incomplete, or inaccurate.

**Examples**: - Missing AI impact assessments required by regulation - Inadequate documentation of risk management processes - Insufficient evidence of bias testing and mitigation - Incomplete records for audit and inspection

**Potential Impacts**: - Regulatory findings and non-compliance notices - Delays in approvals or certifications - Denial of regulatory benefits or protections - Need for expensive remediation efforts - Legal exposure and liability

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 5.3 Cross-Jurisdictional Compliance Challenges

**Risk Description**: AI system operates across multiple jurisdictions with conflicting or complex regulatory requirements.

**Examples**: - Deploying AI globally with different privacy regimes (GDPR vs. other laws) - Conflicting requirements between federal and provincial/state laws - Sector-specific regulations overlapping in different ways - International data transfer restrictions for AI training

**Potential Impacts**: - Inability to deploy consistent AI solutions globally - High costs of compliance across jurisdictions - Regulatory uncertainty and changing requirements - Business restrictions in key markets - Complex legal and compliance management

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 5.4 Copyright and IP Infringement from AI Outputs

**Risk Description**: AI-generated content, outputs, or models infringe on third-party intellectual property rights.

**Examples**: - Generative AI producing content substantially similar to copyrighted works - AI models trained on copyrighted material without authorization - AI-generated code incorporating patented algorithms - AI outputs violating trademark or brand guidelines

**Potential Impacts**: - Copyright infringement lawsuits and damages - Forced removal of AI models or outputs - Legal injunctions halting operations - Significant financial liability - Damage to brand and business relationships

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

### Category 6: Operational Risks

These risks relate to system reliability, performance, and business continuity.

#### 6.1 AI System Failure and Downtime

**Risk Description**: AI system experiences technical failures, crashes, or unavailability causing business disruption.

**Examples**: - Model crashes due to unexpected input data - Infrastructure failures bringing down AI services - Cloud service provider outages affecting AI systems - Software bugs or version incompatibilities causing failures

**Potential Impacts**: - Business process interruptions - Lost revenue from service unavailability - Customer dissatisfaction and churn - Reputation damage from unreliable systems - Cost of emergency fixes and recovery

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 6.2 Degraded Model Performance

**Risk Description**: AI model performance decreases below acceptable thresholds, producing inaccurate or unreliable outputs.

**Examples**: - Accuracy dropping below business requirements - Increased false positive rates in production - Response times exceeding service level agreements - Model outputs becoming inconsistent or unpredictable

**Potential Impacts**: - Poor user experience and customer dissatisfaction - Business decision-making based on flawed information - Revenue losses from ineffective AI applications - Need for costly model retraining or replacement - Erosion of trust in AI capabilities

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 6.3 Inadequate Human Oversight

**Risk Description**: Insufficient human monitoring, review, or intervention in AI systems operating autonomously.

**Examples**: - AI making critical decisions without human review - No monitoring systems alerting to AI performance issues - Automated processes without fallback to human operators - Lack of escalation procedures for AI failures

**Potential Impacts**: - Costly errors going uncorrected - Safety hazards from autonomous AI failures - Regulatory non-compliance with human oversight requirements - Loss of control over business processes - Legal liability for AI-caused damages

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 6.4 Workflow Disruption from AI Integration

**Risk Description**: Integration of AI systems disrupts established business processes, creating chaos or inefficiency.

**Examples**: - Employees confused by new AI workflows - Existing processes breaking due to AI integration - Reliance on AI preventing fallback to manual processes - Technical integration issues causing system failures

**Potential Impacts**: - Productivity losses and operational inefficiency - Employee resistance and decreased morale - Customer service degradation - Failed implementation projects - Financial losses from disrupted operations

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

### Category 7: Human Impact and Safety Risks

These risks relate to potential harm to individuals, groups, or society from AI systems.

#### 7.1 Safety Risks from AI Decisions

**Risk Description**: AI system makes decisions that could cause physical, psychological, or financial harm to individuals.

**Examples**: - Medical AI providing incorrect diagnosis leading to harm - Autonomous vehicle AI making unsafe navigation decisions - Financial AI recommending investments resulting in significant losses - Emergency response AI failing to route resources appropriately

**Potential Impacts**: - Physical injury or death - Severe financial harm to individuals - Legal liability and lawsuits - Regulatory shutdowns of unsafe systems - Criminal prosecution in severe cases

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 7.2 Psychological Harm from AI Interactions

**Risk Description**: AI system interactions cause emotional distress, manipulation, or psychological harm to users.

**Examples**: - AI chatbot for mental health providing harmful advice - Social media AI amplifying negative content causing emotional distress - Gaming AI designed to maximize engagement leading to addiction - AI impersonating loved ones in deceptive ways

**Potential Impacts**: - Psychological trauma and mental health impacts - User complaints and litigation - Regulatory scrutiny and intervention - Reputation damage from harm allegations - Class action lawsuits

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 7.3 Employment and Economic Displacement

**Risk Description**: AI automation eliminates jobs or reduces economic opportunities for workers.

**Examples**: - AI chatbots replacing customer service staff - Automated decision-making reducing need for human analysts - AI-driven process automation eliminating manual roles - Outsourcing enabled by AI reducing local employment

**Potential Impacts**: - Employee layoffs and job losses - Community economic disruption - Labor disputes and union conflicts - Negative public perception and backlash - Regulatory intervention on automation

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 7.4 Social Manipulation and Misinformation

**Risk Description**: AI systems amplify, spread, or generate false or misleading information influencing public opinion or behavior.

**Examples**: - Deepfakes creating convincing but false video content - AI-generated disinformation spreading on social media - Recommendation algorithms creating echo chambers and polarization - Chatbots impersonating public figures to spread misinformation

**Potential Impacts**: - Public deception and manipulation - Democratic process interference - Social unrest and polarization - Regulatory crackdown on AI companies - Criminal liability for deliberate disinformation

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

### Category 8: Third-Party and Vendor Risks

These risks relate to reliance on external AI systems, services, or providers.

#### 8.1 Third-Party AI Vendor Security Breach

**Risk Description**: Third-party AI vendor experiences security incident compromising your data or exposing you to risks.

**Examples**: - Cloud AI platform provider suffers data breach - AI tool vendor hacked exposing your customer data - Outsourced model training service compromised - API provider experiencing security incident

**Potential Impacts**: - Your data exposed in vendor breach - Regulatory liability for third-party security failures - Customer notification and remediation costs - Reputation damage from association with breach - Need to find alternative vendors quickly

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 8.2 Vendor Lock-In and Dependency

**Risk Description**: Heavy reliance on single AI vendor creates vulnerability to price increases, service changes, or vendor failure.

**Examples**: - Entire AI infrastructure dependent on one cloud provider - Proprietary models impossible to migrate to alternatives - Vendor changing terms or pricing dramatically - AI vendor going out of business or discontinuing service

**Potential Impacts**: - Sudden cost increases with no alternatives - Forced migration at high expense - Service disruptions from vendor issues - Loss of competitive flexibility - Business continuity risks

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 8.3 Insufficient Vendor Compliance

**Risk Description**: Third-party AI vendors fail to meet required compliance standards, passing risk to your organization.

**Examples**: - AI vendor not ISO 42001 certified when required - Vendor fails to comply with data protection regulations - Third-party not conducting required impact assessments - Vendor using unethical practices in model development

**Potential Impacts**: - Compliance failures attributed to your organization - Regulatory liability for vendor non-compliance - Contractual breach and legal disputes - Reputation damage from vendor associations - Need for rapid vendor replacement

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

#### 8.4 Unclear Allocation of Responsibilities

**Risk Description**: Ambiguous or disputed responsibility for AI risks between your organization and third-party vendors.

**Examples**: - Unclear contract terms about data ownership - Disagreement about who handles AI incidents - Confusion about regulatory compliance obligations - Shared AI systems with unclear accountability

**Potential Impacts**: - Gaps in risk mitigation leaving exposures - Legal disputes over liability - Regulatory confusion and non-compliance - Blame-shifting during incidents - Inability to enforce vendor commitments

| Impact Score | Likelihood Score | Risk Score | Risk Level | Controls Required | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

## Additional Risk Categories

Use these sections to document risks specific to your organization, industry, or context.

### Industry-Specific Risks

Document risks particular to your industry sector (e.g., healthcare, finance, manufacturing).

| Risk Description | Impact | Likelihood | Risk Score | Controls | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

### Organizational-Specific Risks

Document risks unique to your organizational context, capabilities, or constraints.

| Risk Description | Impact | Likelihood | Risk Score | Controls | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

### Emerging and Unknown Risks

Document risks that are emerging, uncertain, or currently unknown but worth monitoring.

| Risk Description | Impact | Likelihood | Risk Score | Controls | Owner | Target Date | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | [ ] / [ ] / [x] |

## Risk Treatment and Controls

For each identified risk, document your treatment approach and controls.

### Control Categories

Controls fall into these categories:

1. **Preventive**: Stop risks from occurring
2. **Detective**: Identify risks when they occur
3. **Corrective**: Mitigate impact after occurrence
4. **Compensatory**: Alternative means when primary controls fail

### Example Control Strategies

For each risk category, consider these control approaches:

**Bias and Fairness**: - Diversity in training data - Bias testing and monitoring - Fairness metrics and auditing - Inclusive development processes

**Security and Privacy**: - Access controls and authentication - Data encryption and anonymization - Security monitoring and incident response - Vendor security assessments

**Transparency**: - Explainability features and documentation - User disclosure and communication - Audit trails and logging - Model documentation and provenance

**Data Quality**: - Data validation and quality checks - Data lineage and provenance tracking - Monitoring for data drift - Data governance frameworks

**Regulatory Compliance**: - Impact assessments and documentation - Legal and compliance reviews - Monitoring regulatory changes - Vendor compliance requirements

**Operational**: - System monitoring and alerting - Human oversight and intervention - Backup and recovery procedures - Change management processes

**Human Impact**: - Safety testing and validation - Harm monitoring and incident response - User feedback and redress mechanisms - Ethical review processes

**Third-Party**: - Vendor due diligence and assessments - Contract terms and SLAs - Compliance requirements for vendors - Diversification and alternatives

## Summary and Action Plan

### Overall Risk Profile

Calculate your overall risk exposure:

| Risk Level | Count | Percentage |
| --- | --- | --- |
| Extreme (20-25) | \_\_\_ | \_\_\_ % |
| High (15-19) | \_\_\_ | \_\_\_ % |
| Medium (10-14) | \_\_\_ | \_\_\_ % |
| Low (5-9) | \_\_\_ | \_\_\_ % |
| Minimal (1-4) | \_\_\_ | \_\_\_ % |
| **Total Risks** | \_\_\_ | 100% |

### Priority Actions

List top 10 highest-priority risks requiring immediate attention:

| Priority | Risk ID | Risk Description | Risk Score | Owner | Target Date |
| --- | --- | --- | --- | --- | --- |
| 1 | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ |
| 2 | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ |
| 3 | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ |
| 4 | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ |
| 5 | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ |
| 6 | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ |
| 7 | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ |
| 8 | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ |
| 9 | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ |
| 10 | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ |

### Resource Requirements

Estimate resources needed for risk treatment:

* **Budget Required**: $ \_\_\_
* **Personnel Time**: \_\_\_ hours
* **Timeline**: \_\_\_ months to complete priority actions
* **External Support Needed**: Yes / No (specify: \_\_\_)

## Review and Approval

| Role | Name | Signature | Date |
| --- | --- | --- | --- |
| Risk Owner | \_\_\_ | \_\_\_ | \_\_\_ |
| AI Governance Lead | \_\_\_ | \_\_\_ | \_\_\_ |
| Management Representative | \_\_\_ | \_\_\_ | \_\_\_ |
| ISO 42001 Auditor (if applicable) | \_\_\_ | \_\_\_ | \_\_\_ |

## Document Control

| Version | Date | Changes | Author |
| --- | --- | --- | --- |
| 1.0 | \_\_\_ | Initial creation | \_\_\_ |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ |
| \_\_\_ | \_\_\_ | \_\_\_ | \_\_\_ |

**Next Review Date**: \_\_\_  
**Retention Period**: 7 years or as per regulatory requirements

## Appendix: Risk Assessment Methodology

This risk register follows ISO 42001 requirements for AI risk management, informed by:

* **ISO 42001:2023**: AI Management Systems
* **ISO 23894**: AI Risk Management Guidance
* **ISO 31000**: Risk Management Principles and Guidelines
* **ISO 42005**: AI System Impact Assessment

**Key Principles Applied**: 1. Risk-based approach to AI governance 2. Lifecycle perspective (development through decommissioning) 3. Human-centered design considerations 4. Continuous improvement and monitoring 5. Stakeholder engagement and transparency

**Contact for Support**: For assistance using this template or questions about NC-AI standards: - **Website**: kaizenstrategic.ai - **Email**: governance@kaizenstrategic.ai

**License**: This template is released to the public domain. Use, modify, and share freely. Attribution appreciated but not required.

**End of NC-AI-001 Template**

This template provides a comprehensive foundation for AI risk management aligned with ISO 42001. Customize to your organizational needs, but maintain systematic coverage of AI risk categories. Regular review and updates are essential for effective risk management.