

AI Risk Assessment Template

An **AI Risk Assessment Template** is essential for Clause 6 of AIMS (Risk Management). It helps identify, analyze, evaluate, and treat risks related to AI systems.

Here's a **comprehensive template + example** you can include in your training:

1. General Information

- **AI System Name:** _____
- **Process / Function:** _____
- **Date of Assessment:** _____
- **Assessor(s):** _____

2. Risk Identification & Analysis

| Risk ID | Risk Description | Source of Risk | Potential Impact | Likelihood (1–5) | Impact (1–5) | Risk Rating (LxI) | Existing Controls | Risk Owner |
|---------|------------------|----------------|------------------|------------------|--------------|-------------------|-------------------|------------|
|---------|------------------|----------------|------------------|------------------|--------------|-------------------|-------------------|------------|



3. Risk Evaluation & Treatment

| Risk ID | Risk Rating (Before Treatment) | Treatment Option (Avoid / Reduce / Share / Accept) | Planned Actions | Residual Risk Rating | Responsible Person | Timeline |
|---------|--------------------------------|--|-----------------|----------------------|--------------------|----------|
|---------|--------------------------------|--|-----------------|----------------------|--------------------|----------|

4. Monitoring & Review

- Frequency of Risk Review: _____
- Method of Monitoring (e.g., dashboards, audits, bias testing, feedback loops): _____
- Reporting To: _____

Example: AI Recruitment System Risk Assessment

Risk Identification & Analysis

| Risk ID | Risk Description | Source of Risk | Potential Impact | Likelihood (1–5) | Impact (1–5) | Risk Rating (LxI) | Existing Controls | Risk Owner |
|---------|---|-------------------------|--|------------------|--------------|-------------------|---|---------------------|
| R1 | Algorithmic bias leading to unfair hiring decisions | Training data imbalance | Reputational damage, legal non-compliance, employee distrust | 4 | 5 | 20 (High) | Data pre-processing, fairness algorithm | AI Development Lead |

| | | | | | | | | |
|----|--|-----------------------|---|---|---|------------|-----------------------------|-----------------------|
| R2 | Data privacy breach from AI system | Insecure data storage | Regulatory fines, loss of stakeholder trust | 3 | 5 | 15 (High) | Encryption, access controls | IT Security Officer |
| R3 | System downtime during peak recruitment season | Cloud provider outage | Business disruption, lost revenue | 2 | 4 | 8 (Medium) | Vendor SLA, backup servers | IT Operations Manager |

Risk Evaluation & Treatment

| Risk ID | Risk Rating (Before Treatment) | Treatment Option | Planned Actions | Residual Risk Rating | Responsible Person | Timeline |
|---------|--------------------------------|------------------|---|----------------------|----------------------|----------|
| R1 | 20 (High) | Reduce | Implement regular bias audits; train HR staff to spot anomalies | 10 (Medium) | HR Manager & AI Lead | 6 months |
| R2 | 15 (High) | Share | Outsource data hosting to compliant cloud provider with stronger security | 6 (Low) | IT Security Officer | 3 months |
| R3 | 8 (Medium) | Accept | Maintain existing vendor SLA; implement downtime alert system | 8 (Medium) | IT Ops Manager | Ongoing |



✓ This template gives both a **blank format** for learners to use and a **worked example** for clarity.