AIHR | ACADEMY TO INNOVATE HR

// AIHR Resource

AI Risk Assessment Process

GUIDE

The AI Risk Assesment Process

As AI becomes more integrated into HR processes, ensuring its responsible and ethical use is critical. While AI can streamline hiring, performance management, and employee engagement, it also introduces risks—ranging from biased decision-making to data security concerns. A structured risk assessment process helps HR teams proactively identify, mitigate, monitor, and audit AI-related risks to maintain fairness, compliance, and trust in AI-driven systems.

Step 1: Identify risks

- Conduct a thorough review of AI tools currently used in HR. Identify areas where they could fail, such as prediction inaccuracies or lack of transparency in decision-making.
- Involve employees, HR professionals, and technical teams in identifying risks. For example, employees might flag concerns about how their data is used, while technical teams can highlight risks related to system vulnerabilities.
- Anticipate potential risks by considering hypothetical scenarios, such as an AI tool rejecting candidates based on nonrelevant characteristics or an employee's data being leaked due to inadequate security measures.

OUTCOME

A list of potential risks, their severity, and likelihood of occurrence

Tip

If you'd like a personalized report on the potential risks of AI in your HR processes, check out our AI in HR Risk Assessment tool.

Step 2: Mitigate risks

- For identified risks, outline actions to mitigate high potential risks that are likely to occur or have a big business impact.
- Proactively address known and hypothetical risks inherent to the use of AI technology, as a priority. For example, ensure systems are trained on diverse, representative data sets and incorporate fairness algorithms to minimize bias.
- Set up safeguards such as human oversight for high-stakes decisions. For example, while AI might rank candidates, HR professionals should review and validate final hiring decisions.
- Create policies to govern AI usage in HR. These should address data privacy, acceptable use cases, and accountability for decision-making.
- Educate HR teams on how to use AI responsibly and how to interpret and act on AI-driven insights.

OUTCOME

A list of actions to mitigate risks proactively or reactively, along with a description of how they are monitored

Step 3: Monitor risks

- Put mechanisms in place to monitor risks that have been identified and where mitigation strategies and actions are in place. For example, regular reviews and reporting on specific risks.
- Integrate AI risk monitoring into the broader risk reporting process to ensure cross-functional visibility.
- Collect feedback from employees and HR professionals who interact with AI systems. This helps identify risks that may not be apparent from data alone.
- Set up a schedule to evaluate the AI system's outputs. For example, review whether recruitment tools consistently recommend diverse and qualified candidates.
- Monitor external factors such as new regulations or industry trends that could introduce new risks or affect existing mitigation strategies.

OUTCOME

A regular schedule of risks that are tracked, monitored, and reported on in the right forums

Step 4: Audit

- Establish a regular audit cadence to evaluate AI risks holistically.
- Review the effectiveness of risk mitigation efforts. If a strategy isn't delivering the desired results, adjust or replace it.
- Evaluate AI systems for compliance with ethical standards, legal regulations, and organizational policies. For example, audit whether AI decisions are explainable and traceable.
- Maintain detailed records of audit outcomes, including identified risks, mitigation steps, and any changes made. Share these reports with relevant stakeholders to promote accountability and transparency.
- Based on audit findings, refine the risk management process to address gaps and incorporate best practices.

OUTCOME

An audit report and schedule to address any gaps

Case Study: Navigating the Risks of AI Misinterpretation at TechSphere

If you'd like to see the AI risk assessment process in action, here's a case study showcasing how a fictional company identified, mitigated, monitored, and audited AI-related risks to ensure ethical and responsible use.

techsphere

BACKGROUND

TechSphere, a multinational corporation, introduced an AI-driven platform to assess and improve employee engagement by analyzing survey responses and sentiment data. However, some employees expressed concerns that their feedback was being misinterpreted or overly generalized by the AI, leading to inaccurate engagement strategies.

Step 1: Identify risks

TechSphere's HR team, alongside employees and technical experts, identified several risks in the AI tool:

- The risk of misinterpreting employee sentiment due to limited context in survey responses
- The lack of personalization in the AI's analysis, which could lead to generalized engagement recommendations
- Concerns about the transparency of how the AI-generated engagement insights

Step 2: Mitigate risks

To address these concerns, TechSphere:

- Improved the AI tool's natural language processing (NLP) capabilities to better understand nuanced employee feedback.
- Introduced a hybrid approach where AI insights were complemented by human interpretation, ensuring a more personalized approach to employee engagement.
- Created a transparent communication strategy, informing employees about how their feedback was being used and interpreted by AI.

Step 3: Monitor risks

TechSphere implemented continuous feedback loops, asking employees to assess whether the AI-driven engagement strategies were accurately reflecting their needs and concerns. They also reviewed AI-generated recommendations to ensure they were consistent with company values.

Step 4: Audit

A quarterly audit was conducted to assess the effectiveness of AI in improving employee engagement. The audit revealed that while the AI tool had improved engagement in some areas, further adjustments were needed to enhance sentiment analysis accuracy and inclusivity.

TechSphere's proactive approach to monitoring and refining the AI tool improved its accuracy in assessing employee engagement, ensuring that the insights it provided were more relevant and personalized to employee needs.