TechTarget
Search
Enterprise AI

AI risk management checklist

RISK CATEGORY	CHECKLIST ITEM	NEXT STEPS
1. TECHNICAL RISKS	Ensure data quality	• Validate and clean all training data before use. • Implement data versioning to track changes over time. • Flag or remove incomplete or biased data sets.
	Defend against threats	• Conduct regular red team exercises to discover security vulnerabilities. • Apply encryption for AI model data at rest and in transit. • Test models against prompt injection and model extraction attacks.
	Address model explainability	• Deploy SHAP or LIME tools for high-stakes decisions. • Document model logic for auditors and regulatory bodies. • Make explainability reports available to relevant stakeholders.
2. OPERATIONAL RISKS	Validate system integration	• Test AI system compatibility with the existing IT infrastructure before deployment. • Define and document intersection points between AI and human workflows. • Perform regression testing after updates or infrastructure changes.
	Monitor for model drift	• Track model performance metrics on a continuous basis. • Retrain models when performance falls below defined thresholds. • Use dashboards and alerts to flag deviations from expected behavior.

	Establish incident response	• Create a documented plan for AI system failures and errors. • Define escalation paths and assign incident owners. • Conduct post-incident reviews and feed learnings back into system updates.
3. ETHICAL RISKS	Audit for bias and fairness	• Run regular bias audits across training data and model outputs. • Test model outputs across different demographic groups for discriminatory patterns. • Document findings and take corrective actions.
	Embed privacy-by-design	• Minimize and anonymize personal data used in AI model training. • Apply data protection measures at every stage of the AI lifecycle. • Conduct data protection impact assessments (DPIAs) for high-risk systems.
	Assign accountability	• Designate a named owner for each AI system. • Require human signoff on high-stakes automated decisions. • Maintain clear records of who approved AI decisions and when.
4. REGULATORY RISKS	Maintain data protection compliance	• Identify applicable regulations (e.g., GDPR, HIPAA) for each AI system. • Document lawful bases for data processing. • Conduct annual compliance reviews and update practices as laws evolve.
	Align with AI-specific frameworks	• Map AI systems against the NIST AI RMF or ISO 42001 requirements. • Assess whether systems qualify as high-risk under the EU AI Act. • Engage legal counsel for jurisdictions with emerging AI legislation.

	Keep audit-ready documentation	• Maintain records of model versions, training data and decisions made. • Store compliance evidence in a central, accessible repository. • Schedule periodic third-party audits for critical AI systems.