EXECUTIVE BRIEF

What Is an AI Risk Register? A Practical Guide to Tracking and Managing AI Risk

Learn what an AI risk register is, what it should contain, how it differs from an AI inventory, and how organizations use it to identify, assess, treat, monitor, and document AI risk.

IN THIS BRIEF

- What Is an AI Risk Register?
- Inherent risk
- Residual risk
- Treating the inventory as the risk register
- Giving each AI system only one overall risk score

By F. Jay Hall and Stephan Pochet · GRC Careers · August 15, 2026
Source: **ai-governance-jobs.com**

EXECUTIVE SUMMARY

Learn what an AI risk register is, what it should contain, how it differs from an AI inventory, and how organizations use it to identify, assess, treat, monitor, and document AI risk.

KEY TAKEAWAYS

- An AI risk register is a living record of identified risks associated with an organization's AI systems and uses.
- It is different from an AI System Inventory, which tells you what AI systems exist, and an AI Policy Register, which tracks the governance policies that apply to them.
- A useful AI risk register assigns every material risk a named owner, rating, treatment decision, monitoring approach, and review status.
- The register should evolve throughout the AI lifecycle. It is not a one-time compliance worksheet.
- NIST's AI Risk Management Framework emphasizes continuous identification, measurement, management, documentation, accountability, and monitoring of AI risks. A risk register is one practical way organizations can operationalize those activities.
- ISO/IEC 42001 similarly calls for a structured management approach that includes AI risk assessment, risk treatment, monitoring, and continual improvement.
- For organizations subject to the EU AI Act, Article 9 requires a documented and continuously maintained risk-management system for high-risk AI systems. The law does not require an artifact specifically named an "AI risk register," but a well-designed register can provide important evidence of how the process is being managed.

WHAT THIS BRIEF COVERS

What Is an AI Risk Register?. An AI risk register is a structured record used to identify, assess, assign, treat, monitor, and document risks associated with artificial intelligence systems.

Inherent risk. Inherent risk is the level of risk before considering the effect of controls or mitigation measures.

Residual risk. Residual risk is what remains after controls and treatment measures have been applied.

Treating the inventory as the risk register. Knowing an AI system exists does not tell you what risks it creates.

Giving each AI system only one overall risk score. One system may simultaneously create privacy, security, fairness, performance, vendor, legal, and human-oversight risks.

Assigning risk to a committee. "AI Governance Committee" is not a useful entry in the Risk Owner field.

Recording inherent risk but not residual risk. Governance needs to show whether controls actually changed the organization's exposure.

Recording mitigation with no evidence. "Human review implemented" is not enough.

Never updating the register. A beautifully designed risk register that reflects last year's system is worse than a simple register that people actually maintain.

Turning the register into compliance theater. The purpose is not to produce an impressive spreadsheet.