

# Essential Tips for AI Risk Management, Security, and Governance

By Boomi

The [agentic AI revolution](#) isn't coming, it's already here. Businesses are relying on AI for automation and decision-making, with Gartner predicting that [33% of enterprise software will include agentic AI by 2027](#). AI agents are transforming how organizations operate by improving integration initiatives, surfacing mission-critical insights, and automating documentation.

However, the widespread adoption of agentic AI also creates new challenges in governance, privacy, and compliance. As AI agents proliferate across departments, that unmanaged sprawl can cause dangerous security gaps and operational inefficiencies. Fragmented systems and poor oversight are escalating data privacy risks as AI is increasingly used to process sensitive information. Added to this, is the fact that traditional compliance frameworks are often incompatible with AI systems that make autonomous decisions without clear audit trails.

So, how can you take advantage of the power of agentic AI without exposing your organization to hackers and regulatory penalties?

This blog post reveals the practical AI risk management strategies that let you innovate with confidence and achieve a safe and [responsible AI](#) deployment.

## AI Risk Management Fundamentals

To build a successful AI risk management program, start by implementing [NIST's AI Risk Management Framework \(AI RMF\)](#) as your foundation. This is a standardized set of guidelines and controls designed to mitigate AI-specific risks. Its four core components are:

- **Govern:** Build a culture of risk management by establishing oversight systems and policies that align AI systems with your priorities and compliance requirements.
- **Map:** Document your AI ecosystem's entire landscape, including use cases, stakeholder impacts, functionality, and potential blind spots before systems go live.
- **Measure:** Set up testing protocols and key performance indicators (KPIs) to quantify system behavior, evaluate trustworthiness, and track new risks as AI evolves.
- **Manage:** Take action on identified concerns by putting safeguards in place and creating response plans for failures.

Your enterprise must also have strong [software integration](#) capabilities to allow you to centrally manage AI agents and track the flow of data between systems. An [integration platform as a service \(iPaaS\)](#) grants unified visibility across [AI implementations](#), letting you instantly detect and block unauthorized model deployments as well as enforce consistent governance policies.

## Identifying Critical Generative AI Risks

Beyond general cybersecurity threats and compliance vulnerabilities, your risk management strategy must also identify and address the unique risks posed by AI, including:

- **Hallucinations:** AI can generate convincing but entirely fabricated information. Combat this with rigorous fact-checking processes that validate outputs against trusted sources.
- **Data Exposure:** Machine learning models can inadvertently memorize and later reproduce sensitive information from training data, creating privacy risks. Prevent breaches by continuously monitoring for personally identifiable information (PII) and using techniques such as data masking or data anonymization in both training data sets and system outputs.
- **Network Weaknesses:** AI's complex API ecosystems and integration requirements create expanded attack surfaces with vulnerabilities that can be difficult to spot due to the black-box nature of their models. Address these risks by implementing zero-trust architecture principles, regular penetration testing, and comprehensive API protection layers that defend against unauthorized access attempts.
- **Intellectual Property Concerns:** Manage property rights through clear usage policies that define ownership of AI-generated content and monitor outputs to detect potential copyright infringement issues before they escalate.
- **Supply Dependencies:** Mitigate third-party risks by thoroughly vetting all external components, models, and data sources that power your AI systems, and establishing contingency plans for potential disruptions.

## Governance Tips for Effective AI Risk Management

Without a strong cross-functional governance structure, AI risk management becomes siloed and reactive, allowing undetected risks to spread across your business.

Form an interdepartmental AI risk committee with explicitly defined responsibilities and direct reporting lines to executive leadership. A diverse assessment team should include technical experts, legal counsel, ethics specialists, and domain practitioners to measure risks from multiple perspectives and catch blind spots that a smaller team might miss.

This committee should establish detailed acceptable use policies specifically targeting AI technologies. Technical teams must understand the boundaries for appropriate AI agent deployment throughout your organization. Ensure that these guidelines include comprehensive incident response plans so that your teams can quickly address problems when they arise.

While strong governance structures establish the foundation for AI risk management, translating these policies into practical implementation requires a comprehensive framework. The following components ensure that your governance committee's directives can be systematically applied across all AI deployments within your organization:

## AI Risk Assessment Framework:

- **Documentation:** Create detailed profiles for each AI system that describe their intended purposes, operational contexts, and known limitations, ensuring all stakeholders understand both capabilities and constraints.
- **Taxonomy:** Develop standardized classification systems for AI use cases. This enables consistent risk evaluation across similar applications and supports knowledge transfer between teams.

- **Prioritization:** Gauge the potential impacts of AI vulnerabilities by considering both the likelihood of occurrence and the severity of the consequences. Address risks that score high in both categories first, while maintaining awareness of emerging threats.
- **Connectivity:** Use advanced data mapping tools to trace risk dependencies across interconnected systems, identifying how failures in one area might cascade through your technology ecosystem.
- **Monitoring:** Maintain vigilance with regular risk assessments. Evaluate AI systems against thresholds and document exceptions for committee review. For critical issues, design tiered escalation paths and remediation procedures. Connect these governance policies to your technical infrastructure by deploying automated tools that monitor API usage and enforce authentication requirements.

## Expert Measurement Techniques for AI Risks

To quantify AI risks, select context-appropriate metrics that align with your specific AI applications. For example, an AI agent responsible for processing medical records would need to preserve data privacy according to the requirements of the Health Insurance Portability and Accountability Act (HIPAA). On the other hand, a service chatbot would be exposed to the risks of handling sensitive customer information and require completely different risk measurement techniques.

Implement structured testing protocols, including red-teaming and adversarial testing, to thoroughly assess system vulnerabilities. Building on these findings, analyze how AI systems perform across different demographic groups to evaluate fairness and identify potential biases in training data that might affect outputs.

For effective risk management over time, document all measurements in standardized formats that enable meaningful trend analysis. This documentation should include detailed metadata about testing conditions and model versions that can be fed into analytics platforms to power real-time risk dashboards. These dashboards provide stakeholders with much-needed visibility into key risk indicators, visualize trends, and highlight anomalies, creating a continuous feedback loop for risk mitigation.



## Proactive Strategies for Managing AI Risks

Once you've identified and assessed potential AI risks through your governance framework, the next critical step is implementing effective mitigation strategies. A comprehensive approach to AI risk management requires not just detection but also decisive action. Let's take a look at the strategies your organization needs to respond swiftly to emerging threats and maintain system integrity across your AI deployments:

- **Mitigation Plans:** Using the risk scores you created during prioritization, develop tiered response plans for each level of severity. With these plans in place, your business can quickly activate appropriate countermeasures and resolve incidents immediately.
- **Continuous Monitoring:** Establish comprehensive protocols that combine automated surveillance tools with human expertise to ensure complete oversight of AI systems and early detection of anomalies.
- **Deactivating Rogue AIs:** Create specific procedures for safely shutting down or isolating problematic AI systems when necessary, preventing minor issues from escalating into major incidents.
- **External Compliance Checks:** Implement third-party risk assessments for pre-trained models and components to ensure that external AI components meet your organization's security standards before integration.
- **Automated Security:** Leverage advanced automation capabilities to rapidly respond to emerging threats, enabling immediate containment and remediation with minimal human intervention.

## Preparing for Evolving AI Risk Landscapes

AI threats are constantly shifting and morphing, requiring organizations to develop fluid security postures. Perform recurring security research to keep your internal frameworks up-to-date with industry and regulatory developments. Cultivate relationships with AI security resources and communities that provide early warnings about the latest vulnerabilities and emerging threats. Supplement these insights with real-world simulations and tabletop exercises that test your AI incident response capabilities. Set up internal knowledge-sharing mechanisms to spread lessons learned throughout your organization.

To simplify the task of future-proofing your company's AI risk management, partner with Boomi, the leading integration platform as a service (iPaaS).

## Leveraging Boomi for Secure AI Implementation

Boomi's suite of solutions provides the functionality organizations need to implement secure, responsible AI systems at scale. By efficiently connecting disparate systems, streamlining data management, and securing interfaces, Boomi provides transparency and control for your digital assets. Here are the key capabilities Boomi offers for building trusted AI implementations:

- **Centralization:** Use Boomi's intelligent integration platform to unify AI security management across distributed environments. Consolidate security controls into a single pane of glass and simplify your AI governance and monitoring.
- **Data Quality:** Prevent AI failures due to inadequate data preparation by employing Boomi DataHub capabilities. With DataHub, you can easily clean, mask, and address data quality issues to ensure your information is ready for training AI agents.
- **Interface Protection:** Deploy Boomi API management tools to secure the connections between AI agents and data sources, controlling access while maintaining detailed audit trails of all interactions.

- **Workflow Enhancement:** Create automated workflows and rapidly develop applications for continuous monitoring and incident response. The platform's low-code visual workflow designer is intuitive, allowing you to roll out complex procedures with ease.
- **Scalable Architecture:** Boomi features a cloud-native architecture allowing your security measures and policy enforcement systems to grow alongside your AI implementations, without losing performance.

## Boomi Agentstudio's Solutions for AI Risk Management Challenges

At the heart of Boomi's features for AI risk management is Agentstudio, a specialized platform designed to help you build, govern, and orchestrate AI agents securely. Agentstudio addresses the most pressing challenges enterprises face when launching AI projects: security vulnerabilities, oversight gaps, and operational complexity. Two of its core components are:

- **Mitigation Plans:** Using the risk scores you created during prioritization, develop tiered response plans for each level of severity. With these plans in place, your business can quickly activate appropriate countermeasures and resolve incidents immediately.
- **Continuous Monitoring:** Establish comprehensive protocols that combine automated surveillance tools with human expertise to ensure complete oversight of AI systems and early detection of anomalies.
- **Deactivating Rogue AIs:** Create specific procedures for safely shutting down or isolating problematic AI systems when necessary, preventing minor issues from escalating into major incidents.
- **External Compliance Checks:** Implement third-party risk assessments for pre-trained models and components to ensure that external AI components meet your organization's security standards before integration.
- **Automated Security:** Leverage advanced automation capabilities to rapidly respond to emerging threats, enabling immediate containment and remediation with minimal human intervention.

## Agent Designer

The Agent Designer allows you to quickly design, deploy, and test AI agents using pre-built templates while enforcing ethical guidelines. Users can interact with agents using natural language prompts and directly manage API usage.

## Agent Control Tower

Agent Control Tower enhances visibility and prevents agent sprawl by establishing a centralized registry of all AI agents (including third-party systems from other providers, like Amazon Bedrock). Rogue agents can be rapidly identified and disabled using the "kill-switch" functionality.

Trusted for over 25,000 AI agent deployments, Boomi's platform is FedRAMP compliant, ensuring maximum data security. For technology executives navigating the risks of the AI space, Boomi supports innovation while mitigating the risks that could derail AI projects.

**Discover how Boomi Agentstudio can transform your AI risk management strategy.**