Kiteworks

COMPLIANCE BRIEF

Navigate AI Risk Management With NIST AI 600-1 and NIST AI RMF 1.0

Kiteworks Supports Data Protection and Control

NIST AI 600-1 and NIST AI RMF 1.0 are complementary frameworks addressing risks in artificial intelligence systems. NIST AI 600-1 focuses on generative AI risks (GAI), while NIST AI RMF 1.0 provides a broader risk management approach. AI organizations should implement comprehensive risk management throughout the AI life cycle, including governance, mapping, measuring, and managing risks. These frameworks emphasize trustworthiness characteristics like validity, safety, security, and fairness. While voluntary, compliance is crucial for industries handling sensitive data or high-stakes decisions. NIST AI 600-1 supplements NIST AI RMF 1.0 with specific guidance on generative AI risks, such as hallucinations and information integrity issues. Together, they enable responsible and ethical AI system development and deployment across various industries.

Bridge AI Governance and Data Tracking

The Govern function is a foundational element that fosters a comprehensive risk management culture in organizations dealing with AI systems. It establishes processes for anticipating, identifying, and managing risks throughout the AI life cycle and emphasizes the importance of transparent policies, clear accountability structures, workforce diversity, and robust engagement with relevant AI actors. It also addresses managing risks associated with third-party software and data in the AI supply chain. The Kiteworks platform maintains a consolidated activity log that records all interactions with content, including those made by third parties. This log captures views, downloads, uploads, edits, and deletions, along with user IDs, timestamps, and metadata. The Enterprise Connect feature extends this tracking to external repositories, ensuring consistent monitoring of content changes across integrated systems. This thorough record-keeping promotes content provenance and supports intellectual property protection in AI systems.

Comprehensive AI Risk Mapping of Data Interactions and Policies

Establishing context for framing risks related to an AI system and considering the interdependencies of activities and actors throughout the AI life cycle is detailed in the Map function. It enhances an organization's ability to identify risks and broader contributing factors, providing the foundation for the subsequent Measure and Manage functions and informing critical decisions about AI system development and deployment.

Solution Highlights

- Consolidated audit log
- Enterprise Connect
- Customized admin roles
- CISO Dashboard
- SIEM integration

Kiteworks' risk policy framework enables audit logging of events corresponding to specific policies, allowing for detailed review of data usage. Customizable admin roles provide access to comprehensive dashboards, including system-level activity logs, custom reports, and trend graphs. The CISO Dashboard offers geographical insights into data activities, while compliance-specific dashboards summarize tracking data for regulations like GDPR and HIPAA. These features enable organizations to review and document the accuracy, representativeness, and suitability of data used throughout the AI life cycle.

Manage Information Integrity in Risk Management

The Manage function involves allocating resources to address mapped and measured risks, implementing response and recovery plans, and communicating about incidents or events. It leverages information from the previous functions to decrease the likelihood of system failures and negative impacts, while establishing processes for continual improvement and managing emergent risks. The platform maintains a single, consolidated activity log that documents all data interactions, including views, downloads, uploads, edits, and deletions. Kiteworks' real-time SIEM integration enables immediate analysis of security threats and anomalies. The system captures user IDs, timestamps, and IP addresses for each action, facilitating the documentation of training data sources and supporting information integrity throughout the AI life cycle. This thorough logging and integration capability enhances an organization's ability to manage and respond to data risks effectively.

Kiteworks' features support compliance with NIST AI 600-1 and AI RMF 1.0 frameworks, providing robust support for data layer compliance. The platform's consolidated activity logging, real-time SIEM integration, and Enterprise Connect feature enable thorough tracking and monitoring of all data interactions, including those involving third parties. Kiteworks' risk policy framework, customizable admin roles, and compliance-specific dashboards allow organizations to review and document data usage throughout the AI life cycle. These capabilities, combined with strong access controls, facilitate the tracing of data content, support information integrity, and enhance an organization's ability to manage and respond to data risks effectively. By implementing these features, organizations can support responsible and ethical AI system development while maintaining stringent data protection standards.