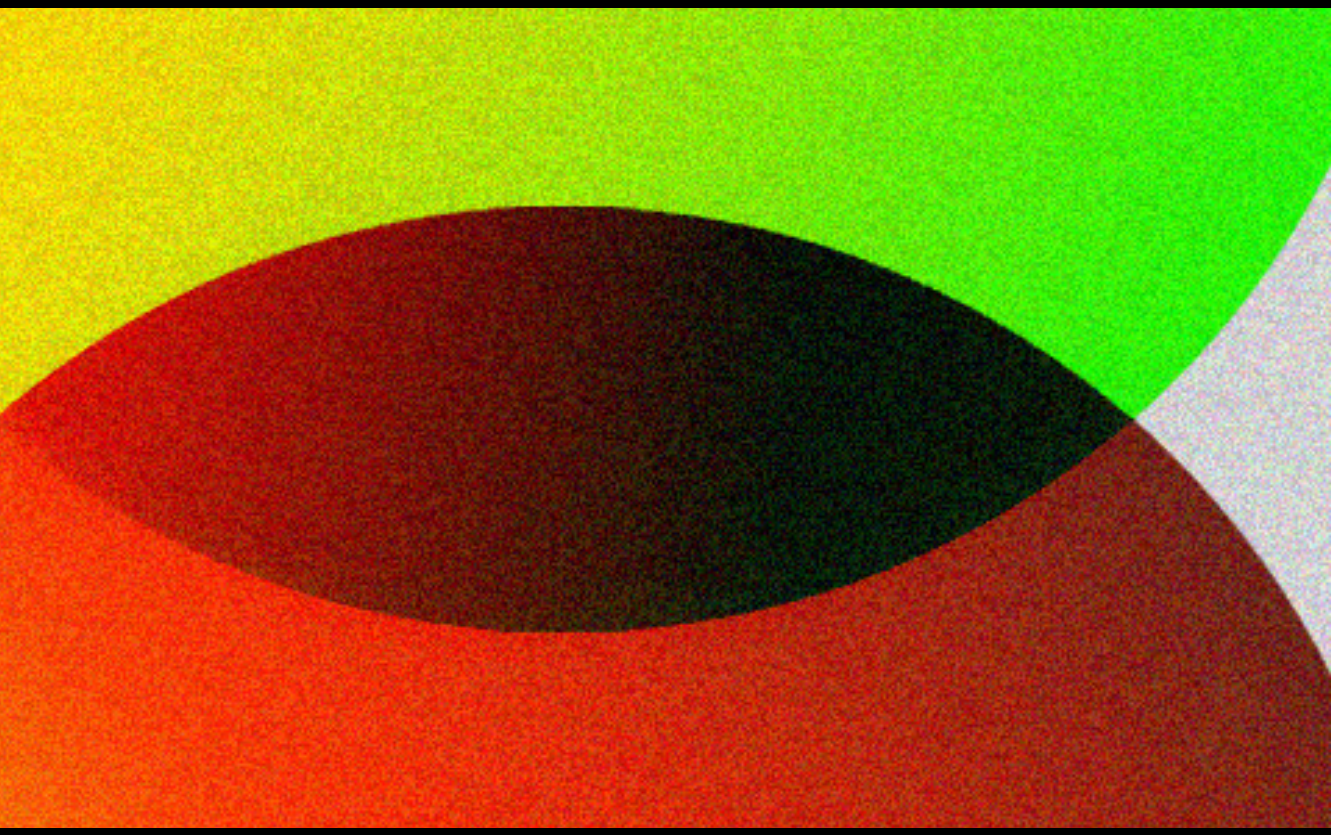
KONTENT.AI



Kontent.ai complies with NIST AI RMF

www.kontent.ai

What is NIST AI RMF and why it matters

The NIST AI Risk Management Framework (AI RMF) is a set of recommendations designed to help organizations manage risks associated with the design, development, deployment, and use of artificial intelligence systems. It emphasizes the importance of governance, mapping, measuring, and managing AI risks throughout the AI system lifecycle.

The AI RMF is significant because it provides a structured approach to AI risk management, ensuring that AI systems are developed and used responsibly, ethically, and with an understanding of the potential impacts on individuals and society. It helps organizations align their AI practices with legal and regulatory requirements, as well as ethical standards, thereby fostering trust and confidence in AI technologies.

Executive summary

The NIST AI RMF offers a playbook with suggested actions for achieving the outcomes laid out in the AI RMF Core, which includes four functions: Govern, Map, Measure, and Manage. These functions provide a comprehensive approach to AI risk management, ensuring that policies, processes, and practices are transparent, effective, and aligned with organizational risk priorities.

- **Govern** – Policies and structures for AI risk management and align them with the legal, ethical, and societal aspects of AI.
- **Map** – Identifies the AI risks, impacts, objectives, stakeholders, data, and scope in a specific application context.
- **Measure** – Assesses the risks and monitors the performance and trustworthiness of the AI system using various methods and metrics.
- **Manage** – Implements and maintains the policies and procedures for managing AI risks throughout the AI lifecycle and provides training and education for the staff and partners.

How to work with this document

This document is intended to guide organizations in implementing AI risk management practices. It is not a checklist but rather a set of voluntary suggestions that can be adapted to various industry use cases or interests. Organizations are encouraged to use the information by incorporating relevant suggestions into their AI risk management strategies.

The document outlines actions and considerations for each sub-category within the AI RMF functions, providing a framework for organizations to document their AI risk management efforts and enhance accountability.

Below is a table for the shared responsibility model of activities to follow NIST AI RMF recommendations to mitigate the risk of using the AI system.

Area	Control	Kontent.ai controls and comments	Kontent.ai recommendations
Govern	Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively.	Kontent.ai ensures compliance with AI legal and regulatory requirements by maintaining an AI system inventory, conducting regular compliance reviews, and documenting processes for measurement and data privacy.	Clients should perform impact assessments and train staff on AI ethics to support transparency and accountability in the usage of AI.
	Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.	Owners of AI risk are defined and have responsibilities across the organization, ensuring separation of risk evaluation for unbiased risk assessment and management.	Similar to Kontent.ai, customers are encouraged to establish ownership over the management of risks related to the usage of AI in the Kontent.ai application.
	Workforce diversity, equity, inclusion, and accessibility processes are prioritized in the mapping, measuring, and managing of AI risks throughout the lifecycle.	Kontent.ai has established policies that prioritize workforce diversity, equity, inclusion, and accessibility in AI risk management, ensuring a broad range of perspectives is considered throughout the AI system lifecycle, from design to monitoring.	Customers are advised to include workforce diversity, equity, inclusion, and accessibility considerations in the AI risk management.
	Organizational teams are committed to a culture that considers and communicates AI risk.	Kontent.ai implements organizational policies that encourage a critical thinking and security-first mindset, ensuring oversight functions are included from the outset of AI system design and promoting effective challenges of AI system decisions to minimize risks.	Kontent.ai encourages customers to build an AI risk-aware culture internally as well.

Area	Control	Kontent.ai controls and comments	Kontent.ai recommendations
Govern	Processes are in place for robust engagement with relevant AI actors.	Established a model documentation inventory system to ensure comprehensive and current AI system documentation, including AI actor contact information, business justification, and stakeholder engagement plans, in line with industry best practices.	Customers are welcome to actively participate in stakeholders' feedback and review the AI system's documentation provided by Kontent.ai to better understand the design, operations, and limitations of the AI system, ensuring alignment with their own risk management policies.
	Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues.	Supply Chain Security Policy that addresses third-party supplier risks, including AI concerns, by setting clear security requirements, conducting regular reviews, and performing audits to ensure compliance.	Customers can request and review SBOM and VEX reports from Kontent.ai to gain insights into third-party components and their associated risks, enhancing their own risk management strategies.
Map	Context is established and understood.	Kontent.ai documents the intended use and potential impacts of AI systems, ensuring compliance with context-specific laws and norms and maintaining transparency throughout the AI lifecycle.	Any use cases utilizing the AI capabilities of Kontent.ai should be documented and discussed.
	Categorization of the AI system is performed.	Defined and documented the tasks and methods used by the AI system, ensuring clarity on the system's capabilities and limitations, and categorizing the system accordingly, whether it's a classifier, generative model, or recommender.	Customers should categorize the AI capabilities of Kontent.ai and include it in the inventory of their AI systems.
	AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.	AI system capabilities and goals are aligned with organizational objectives and benchmarks.	Customers should consider the AI capabilities of Kontent.ai and understand their use cases and goals.

Area	Control	Kontent.ai controls and comments	Kontent.ai recommendations
Map	Risks and benefits are mapped for all components of the AI system, including third-party software and data.	Kontent.ai maintains a comprehensive inventory of all systems, including third-party software, with documented risk assessments and security classifications to manage risks associated with AI components and third-party data usage, ensuring compliance with intellectual property laws and other regulations.	Risk registers of Kontent.ai customers should include AI risks, including those related to the AI capabilities of the Kontent.ai application.
	Impacts on individuals, groups, communities, organizations, and society are characterized.	Built-in moderation and filtering capabilities are in place to mitigate harmful AI behavior.	Based on their use cases, customers should evaluate and characterize the impacts of using the AI capabilities of Kontent.ai.
Measure	Appropriate methods and metrics are identified and applied.	Kontent.ai involves internal experts and independent assessors who were not part of the system's development for regular assessments and updates of AI metrics and controls, incorporating diverse perspectives.	Customers should measure their usage of the AI capabilities of Kontent.ai according to their identified needs and use cases.
	AI systems are evaluated for trustworthy characteristics.	Kontent.ai measures AI system performance against qualitative or quantitative criteria that are similar to the deployment settings, documenting these measures to demonstrate assurance.	Customers should review the correctness of the output to ensure the AI generates correct data.
	Mechanisms for tracking identified AI risks over time are in place.	Tracking mechanisms are established to monitor AI risks over time, allowing for the timely identification of emerging risks.	Monitor and track AI risks concerning the usage of Kontent.ai AI capabilities over time.

Area	Control	Kontent.ai controls and comments	Kontent.ai recommendations
Measure	Feedback about the efficacy of measurement is gathered and assessed.	Feedback mechanisms are in place to evaluate the effectiveness of AI risk measurement methods.	Establish feedback mechanisms to measure and track risks concerning the usage of Kontent.ai AI capabilities.
Manage	AI risks based on assessments and other analytical output from the Map and Measure functions are prioritized, responded to, and managed.	AI risks are prioritized and managed based on comprehensive quantitative risk assessments.	Ensure that all relevant AI risks are managed.
	Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, and documented, and informed by input from relevant AI actors.	Various stakeholders for AI stories guarantee the safeness, efficiency, and performance of AI functionality.	Customers are encouraged to leverage the benefits of AI while minimizing the negative impact by managing risk and implementing relevant controls on their end.
	AI risks and benefits from third-party entities are managed.	All third parties are reviewed by the architecture board, including security review, prior to any integration with Kontent.ai to identify risks and benefits.	Regularly monitor the performance and trustworthiness of pre-trained models and as part of third-party risk tracking.
	Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly.	Risk treatments, response and recovery, and communication plans are documented and reviewed regularly.	Customers should identify, measure, document, and monitor their risk treatments considering the AI capabilities of Kontent.ai.

NIST AI RMF Compliance

Even though the NIST AI RMF is not mandatory for AI solutions, Kontent.ai makes an extra effort to follow these recommendations to implement and provide AI in a secure and responsible way. Also, documenting our AI risk management practices, including but not limited to:

- Legal and regulatory considerations specific to industry and AI applications.
- Standardized documentation policies for AI systems, including information on AI actors, training data, algorithmic methodology, and testing results.
- Policies for measuring AI systems impact risk levels and risk tolerance decisions.

However, customers are also responsible for using Kontent.ai's AI products and services in a way that aligns with their own organizational goals and values, as well as ethical, legal, and social norms and expectations. Therefore, both Kontent.ai and its customers need to follow the best practices given by NIST AI RMF to better manage the risks and impacts associated with AI and their respective roles and responsibilities.

Information in this whitepaper is for informational purposes only and does not constitute legal advice.

About Kontent.ai

Kontent.ai's mission is to help the world's leading organizations achieve an unparalleled return on their content. In the industry's first AI-powered CMS, content teams plan, create, and optimize content and deliver it to any channel—quickly, securely, and flexibly. Kontent.ai is designed to support organizations with exacting governance requirements, often in highly regulated industries and with complex content value chains.

Tight permissions control all operations; enterprise-grade security and privacy keep content safe. With a demonstrated ROI of 320%, Kontent.ai customers, including PPG, Elanco, Zurich Insurance, Cadbury, and Oxford University, benefit from a measurable step change in how their teams operate, increasing content velocity, mitigating risk, and maximizing yield. Kontent.ai is a Microsoft partner, MACH Alliance member, and recognized vendor by Gartner and Forrester. Learn more at: kontent.ai.

Want to see Kontent.ai in action?

Schedule a demo

KONTENT.AI®