

NIST SP AI 100-1 NIST AI Risk Management Framework Compliance Attestation

Issued by: Akka Technologies, Inc.

Prepared by: Michael Nash, Chief Information Security Officer

Date of Attestation: 20 April 2026

Document Classification: Public

Review Cycle: Annual

Introduction

This attestation is issued by Akka Technologies, Inc. ("Akka") to confirm our alignment and compliance posture with respect to the NIST AI Risk Management Framework (NIST AI RMF 1.0), published by the National Institute of Standards and Technology as NIST Special Publication AI 100-1 in January 2023.

Akka is a technology company headquartered in the United States, providing the Akka platform — a reactive microservices and distributed systems toolkit enabling enterprises to build and operate agentic AI applications at scale. Akka adopts the NIST AI RMF as a voluntary, risk-based framework to govern the trustworthy development, deployment, and operation of AI systems across the four core functions: GOVERN, MAP, MEASURE, and MANAGE.

The NIST AI RMF is particularly valued by Akka's US federal, financial services, and enterprise customers, who expect their AI infrastructure providers to demonstrate structured, measurable AI risk management practices consistent with NIST guidance. This attestation documents

Akka's implementation of all 14 controls within the NIST AI RMF 1.0 framework, all assessed at Low residual risk.

This attestation covers the period ending 20 April 2026 and will be reviewed no less than annually.

Scope and Applicability

The NIST AI RMF 1.0 provides voluntary guidance for managing risks to individuals, organisations, and society associated with the development and use of AI systems. It is organised around four core functions that together constitute a comprehensive approach to AI risk management:

GOVERN: Establishing and maintaining organisational structures, policies, processes, and accountability mechanisms for AI risk management.

MAP: Identifying and categorising risks associated with AI systems throughout their lifecycle.

MEASURE: Analysing, quantifying, and tracking AI risks using appropriate methods and metrics.

MANAGE: Prioritising and responding to identified AI risks, including treatment, monitoring, and incident response.

Akka applies the NIST AI RMF to its own AI features and products, to AI-related capabilities exposed through the Akka platform for customer use, and to the governance of AI systems deployed internally. All 14 NIST AI RMF 1.0 controls in Akka's ISMS are in Implemented status with Low residual risk.

Compliance Posture

Akka is fully aligned with the NIST AI RMF 1.0 as of the date of this attestation. This determination is based on the implementation of all 14 framework controls, the operation of an AI governance structure centred on Akka's AI Review Board, and the embedding of AI risk management practices within Akka's broader ISO 27001-aligned ISMS.

GOVERN Function – AI Risk Governance Structure

Akka has established a comprehensive governance structure for AI risk management, operationalising the GOVERN function of the NIST AI RMF:

AI Review Board: Akka operates a formal AI Review Board with CISO-level leadership, responsible for overseeing all AI-related risk decisions, approving new AI system deployments, and ensuring that AI governance policies are maintained and enforced. The Board meets regularly and maintains documented records of its decisions.

AI Policy: Akka maintains a documented AI Policy that establishes principles, roles, responsibilities, and requirements for all AI activities across the organisation. The policy addresses transparency, accountability, human oversight, data governance, and responsible AI practices.

AI Governance Integration: AI governance is integrated into Akka's ISMS, ensuring that AI-specific controls benefit from the same review, audit, and continual improvement processes as broader information security controls.

Roles and Accountability: Clear accountability assignments exist for all AI systems in production, with designated owners responsible for risk management, performance monitoring, and compliance obligations. These assignments are recorded in both the Agent Registry and the ISMS.

Organisational AI Risk Culture: Akka promotes AI risk awareness across the organisation through training, policy communication, and integration of AI risk considerations into product development and operations processes.

MAP Function — AI Risk Identification and Categorisation

Akka's MAP function implementation ensures that AI risks are systematically identified and contextualised:

AI System Inventory: Akka maintains a current inventory of all AI systems and agentic AI capabilities deployed within the platform or used internally, recorded in the Agent Registry. Each entry documents the system's intended purpose, deployment context, potential affected parties, and risk tier.

Risk Context Assessment: For each AI system, Akka conducts a risk context assessment that identifies relevant stakeholders, potential impacts on individuals and society, data and model dependencies, and applicable regulatory obligations. This assessment informs the MAP function's categorisation of AI risks.

Threat and Vulnerability Identification: AI-specific threats — including prompt injection, model drift, adversarial inputs, data poisoning, and hallucination risks — are identified and documented as part of the risk context assessment, drawing on guidance from NIST AI 600-1, OWASP AI, and MITRE ATLAS.

Regulatory Mapping: Akka maps AI system risks to applicable regulatory frameworks including the EU AI Act and ISO/IEC 42001, ensuring that regulatory risk is captured alongside technical and operational risk in the MAP function outputs.

MEASURE Function – AI Risk Analysis and Quantification

Akka's MEASURE function implementation provides quantitative and qualitative analysis of AI system risks:

Performance Metrics and Monitoring: AI systems deployed on the Akka platform are instrumented with performance monitoring covering accuracy, latency, availability, and behavioural consistency. Defined thresholds trigger alerts for investigation and remediation when performance degrades.

Risk Scoring: AI systems in Akka's ISMS are assessed using a risk scoring methodology that evaluates likelihood and impact of identified AI risks, producing residual risk scores used to prioritise treatment actions. All 14 NIST AI RMF controls are at Low residual risk.

Bias and Fairness Measurement: Where AI systems produce outputs that may affect individuals, Akka conducts bias and fairness assessments as part of pre-deployment testing and ongoing monitoring, with results documented and reviewed by the AI Review Board.

Evaluation Testing: AI features undergo structured evaluation testing prior to production deployment, including adversarial robustness testing, boundary condition testing, and performance benchmarking against defined acceptance criteria.

Metrics Reporting: AI risk metrics are reported to the AI Review Board on a regular basis, enabling trend analysis and informed governance decisions. Key metrics include incident rates, performance degradation events, and control effectiveness scores.

MANAGE Function — AI Risk Treatment and Incident Response

Akka's MANAGE function ensures that identified AI risks are appropriately treated, monitored, and responded to:

Risk Treatment: For each AI risk identified in the MAP and MEASURE functions, Akka maintains a documented treatment plan. Risk treatments include technical controls (scope limitation, override mechanisms, monitoring), operational controls (human oversight requirements, approval workflows), and procedural controls (escalation procedures, change management).

AI Incident Response: Akka maintains AI-specific incident response procedures, integrated with the organisation's broader incident response programme. AI incidents are classified by type (performance failure, security incident, safety event, compliance event) and handled through defined response playbooks. Post-incident reviews feed into the MAP and MEASURE functions to improve risk identification and measurement.

Change Management for AI: Material changes to AI systems — including model updates, capability additions, and deployment context changes — trigger a re-evaluation through the MAP and MEASURE functions before being approved by the AI Review Board.

Ongoing Risk Monitoring: AI systems in production are subject to continuous monitoring for risk indicators, with automated alerting and human review processes ensuring that emerging risks are identified and managed in a timely manner.

Supplier AI Risk Management: Akka extends its AI risk management to third-party AI components and GPAI model providers integrated into the platform, conducting due diligence assessments to ensure that upstream AI risks are identified and managed.

ISO/IEC 42001 and EU AI Act Alignment

Akka's NIST AI RMF implementation is reinforced by complementary AI governance frameworks:

ISO/IEC 42001:2023: Akka has implemented all 98 controls of the ISO/IEC 42001 AI Management System standard at Low residual risk. The ISO/IEC 42001 management system provides the organisational infrastructure within which NIST AI RMF functions are operationalised.

EU AI Act Alignment: Akka's 82-control EU AI Act compliance framework aligns the NIST AI RMF's risk management practices with the regulatory requirements of Regulation (EU) 2024/1689, ensuring that US-framework AI risk management translates into demonstrable regulatory compliance for EU operations.

ISO 27001-Aligned ISMS: All AI governance controls are embedded in Akka's ISO 27001-aligned ISMS, providing integrated assurance across information security, privacy, and AI risk domains.

Supporting Evidence

The following evidence supports this attestation:

- Akka ISMS — NIST AI RMF 1.0 control framework, 14 controls, all Implemented at Low risk
- AI Review Board charter and meeting records
- AI Policy (publicly available)

- Agent Registry — AI system inventory and accountability assignments
- AI risk assessments and risk scoring records
- AI performance monitoring metrics and dashboards
- AI incident response procedures and incident logs
- SOC 2 Type II report (available under NDA)
- AWS infrastructure SOC 2 and ISO 27001 documentation
- ISO/IEC 42001 control implementation records

Conclusion

Akka's alignment with the NIST AI RMF 1.0 reflects our commitment to structured, measurable, and continually improving AI risk management. By implementing all four core functions — GOVERN, MAP, MEASURE, and MANAGE — across all 14 framework controls at Low residual risk, Akka provides its customers and stakeholders with strong assurance that AI risks are managed systematically and responsibly.

US federal, financial services, and enterprise customers can rely on Akka's NIST AI RMF alignment as evidence of a mature, risk-aware AI governance programme that meets the expectations of US government guidance and enterprise procurement requirements.

This attestation is available to customers and prospects on request and is subject to annual review. Questions regarding Akka's NIST AI RMF compliance programme should be directed to:

Michael Nash

Chief Information Security Officer

Akka Technologies, Inc.



Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

michael.nash@akka.io

Signed: Michael Nash, CISO, Akka Technologies, Inc.

Date: 20 April 2026