AKKA

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

Network and Information Security Directive 2 Compliance Attestation

Introduction

Directive (EU) 2022/2555 — the Network and Information Security Directive 2 (NIS2) — is the European Union's primary cybersecurity legislation for essential and important entities operating within the EU. It repeals and substantially strengthens the original NIS Directive (2016/1148), significantly expanding its scope, raising the bar for security requirements, and tightening incident reporting obligations. Member States were required to transpose NIS2 into national law by 17 October 2024.

NIS2 applies to organisations operating in sectors designated as essential or important, and to digital infrastructure and service providers — including cloud computing service providers, managed service providers, and providers of online marketplaces, search engines, and social networking platforms — that operate in or provide services to entities in the EU. Akka, as a provider of a SaaS-based reactive microservices and distributed systems platform serving enterprise customers in the EU, aligns with the obligations applicable to digital service providers and managed service providers under NIS2.

This attestation confirms Akka's alignment with the security and governance requirements of NIS2 as of the date stated below. Akka's ISO 27001-aligned Information Security Management System (ISMS) and SOC 2 Type II attestation provide the governance infrastructure underpinning this compliance posture.

Scope

AKKA

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

This attestation covers Akka Technologies, Inc.'s ("Akka") cybersecurity risk management, incident reporting, and supply chain security practices as they pertain to NIS2. In-scope systems and activities include:

Network and information systems: Akka's SaaS platform, supporting cloud infrastructure, internal corporate IT systems, and development environments.

Incident management: detection, analysis, containment, and reporting of cybersecurity incidents affecting Akka's services.

Supply chain security: assessment and management of third-party suppliers and sub-processors that have access to Akka's systems or customer data.

Business continuity: backup, disaster recovery, and resilience capabilities for Akka's platform and operations.

Compliance Posture

Akka maintains 17 controls specifically mapped to NIS2 within its Information Security Management System (ISMS). All 17 controls are in Implemented status. Risk distribution across the control set is as follows:

- 5 controls rated Low risk
- 12 controls rated Medium risk
- 0 controls rated High risk

AKKA

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

Overall NIS2 compliance is assessed as Compliant. The Medium-risk ratings reflect the inherent complexity of operating a distributed SaaS platform across multi-cloud infrastructure, and Akka has implemented compensating and detective controls in each case. Akka's ISMS is aligned with ISO/IEC 27001 and supported by a SOC 2 Type II attestation from an independent auditor, providing external assurance of the effectiveness of Akka's security controls.

Key Controls Implemented

Cybersecurity Risk Management

Akka operates a formal, documented information security risk management programme aligned with ISO/IEC 27001 principles. Risks to network and information systems are identified, assessed, and treated using a structured risk register. Risk owners are assigned for each identified risk, treatment plans are tracked to completion, and the overall risk posture is reviewed at least annually by senior management. Risk assessments are triggered by material changes to systems, services, or the threat landscape in addition to the scheduled review cycle.

Incident Detection and Response

Akka maintains a documented incident response plan covering the full lifecycle of a security incident: detection, triage, containment, eradication, recovery, and post-incident review. Security monitoring is implemented across Akka's infrastructure to detect anomalous activity, unauthorised access attempts, and indicators of compromise. Incidents are classified by severity, and escalation paths are clearly defined. In the event of a significant incident affecting Akka's services or customer data, Akka is prepared to notify affected customers and relevant competent authorities in accordance with NIS2 reporting timelines — early warning within 24 hours, initial notification within 72 hours, and final report within one month.

AKKA

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

Supply Chain Security

Akka applies a structured vendor risk management programme to all third-party suppliers and sub-processors. Prior to onboarding, suppliers are assessed for security posture, and contractual security requirements are imposed in all supplier agreements. Sub-processors handling customer data are required to demonstrate equivalent security standards and are subject to periodic review. Akka maintains a current register of sub-processors and communicates changes to customers in advance. Critical dependencies in Akka's supply chain are identified and subject to enhanced monitoring.

Business Continuity and Resilience

Akka maintains documented business continuity and disaster recovery plans covering its SaaS platform and critical internal systems. Regular backups are performed, tested, and stored with appropriate isolation to protect against ransomware and other destructive attacks. Recovery time and recovery point objectives are defined for critical services, and recovery procedures are tested through tabletop exercises and operational runbooks. Infrastructure resilience is achieved through multi-availability-zone deployments on Akka's cloud infrastructure providers.

Access Control and Cryptography

Access to Akka's systems and platform is controlled on the principle of least privilege. Multi-factor authentication is enforced for access to critical systems and administrative interfaces. Privileged access is time-limited, audited, and subject to enhanced monitoring. Akka applies encryption to data in transit and at rest using current industry-standard cryptographic algorithms. Cryptographic key management procedures govern key generation, storage, rotation, and revocation.

Vulnerability Handling and Patching

AKKA

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

Akka operates a documented vulnerability management programme covering its SaaS platform, supporting infrastructure, and internally developed software. Vulnerability scanning is conducted regularly, and identified vulnerabilities are triaged and remediated in accordance with defined severity-based timelines. Akka maintains a responsible disclosure policy enabling external researchers to report potential vulnerabilities. Critical and high-severity patches are applied on an accelerated schedule, with emergency change procedures available for zero-day threats.

Security Policies and Governance

Akka's information security governance framework includes a suite of policies covering acceptable use, access control, incident management, business continuity, supplier security, cryptography, and vulnerability management. These policies are reviewed and updated at least annually, approved by senior management, and communicated to all relevant personnel. Security awareness training is provided to all staff at onboarding and on a recurring annual basis, with role-specific training for personnel in security-sensitive roles.

Supporting Evidence

The following evidence supports this attestation:

- ISO 27001-aligned ISMS with full risk register, treatment plans, and management review programme
- SOC 2 Type II attestation report from an independent auditor (available under NDA on request)
- Documented incident response plan with defined reporting timelines aligned to NIS2
- Supplier security assessment programme and sub-processor register
- Business continuity and disaster recovery plans with tested recovery procedures

- Vulnerability management programme with tracked remediation metrics
- Security policies reviewed and approved by senior management within the last twelve months
- Annual security awareness training with completion tracking for all staff

Conclusion

Akka Technologies, Inc. attests that, as of the date of this document, its network and information security practices align with the requirements of Directive (EU) 2022/2555 (NIS2 Directive). All 17 NIS2 controls in Akka's ISMS are fully implemented, risk levels are Low or Medium, and no High-risk control gaps exist.

Akka operates as a SaaS provider in the EU market and takes its obligations under NIS2 seriously, maintaining the governance, technical, and operational capabilities required to protect its platform and customers from cybersecurity threats. This attestation is reviewed annually or upon material changes to Akka's security posture or the applicable regulatory framework. It is available to customers, prospects, and competent authorities on request.

Michael Nash

Chief Information Security Officer

Akka Technologies, Inc.

michael.nash@akka.io

Date: 20 April 2026