AKKA

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

Attestation of Compliance with the EU Cyber Resilience Act (CRA)

Issuer: Akka

Date: 2026-04-23

Subject: Compliance with Regulation (EU) 2024/2847 — EU Cyber Resilience Act (CRA), adopted October 2024

Introduction

Akka is a provider of software products with digital elements — including the Akka SDK, platform libraries, and cloud-delivered SaaS services — that are made available in the EU market. The European Union Cyber Resilience Act (CRA), officially adopted in October 2024, establishes comprehensive cybersecurity requirements for products with digital elements throughout their entire lifecycle, from design and development through deployment and end-of-life. Akka is committed to full compliance with CRA obligations as they become applicable under the phased implementation timeline.

Of 105 CRA controls tracked by Akka, 95 are fully implemented. The remaining 10 are Inactive pending the applicability date of the corresponding CRA obligations under the phased timeline (main obligations applicable from December 2027; vulnerability reporting obligations from December 2026). All 105 implemented controls carry a Low risk rating.

Applicability

AKKA

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

The CRA applies to Akka as a manufacturer of software products with digital elements, including:

- The Akka SDK distributed to developers for building agentic AI applications
- Platform components and libraries integrated into customer applications
- The cloud-delivered Akka platform where it incorporates software components

Akka's products are assessed against the CRA's default category requirements (not critical or critical Class I/II products), given their role as developer tooling and platform infrastructure.

Scope of Compliance

1. Security by Design and Default (Article 13)

Akka designs and develops its products following security-by-design and security-by-default principles throughout the Software Development Life Cycle (SDLC). Security requirements are identified and implemented from the earliest design phase. Default configurations are secure out-of-the-box, with unnecessary features disabled by default. Akka's SDLC policy mandates security review gates at design, implementation, and pre-release stages.

2. Vulnerability Identification and Management (Articles 13, 14)

Akka maintains a documented vulnerability management programme covering:

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

- Continuous vulnerability scanning of Akka's platform and product dependencies using Wiz and FOSSA software composition analysis

- A coordinated vulnerability disclosure policy enabling external researchers to report vulnerabilities to security@akka.io

- A vulnerability remediation process with risk-based prioritisation and defined SLAs for critical and high-severity findings

- Tracking of known exploited vulnerabilities in Akka's product components

3. Vulnerability Reporting (Article 14)

Akka maintains procedures for reporting actively exploited vulnerabilities and severe incidents affecting its products to ENISA and relevant national computer security incident response teams (CSIRTs) within the timelines required by CRA Article 14. Internally discovered and externally reported vulnerabilities are triaged and, where they meet CRA reporting thresholds, notified in accordance with the CRA reporting process.

4. Security Updates Throughout the Support Period (Article 13)

Akka provides security updates for its products throughout the defined support period. Critical security patches are developed and released as rapidly as possible following identification of a vulnerability. Customers are notified of security updates through Akka's release notification channels. Updates are delivered in a manner that does not unnecessarily disrupt customer operations.

5. Software Bill of Materials (SBOM) (Article 13)

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

Akka maintains a Software Bill of Materials (SBOM) for its products, documenting all software components, including open-source dependencies. SBOM management is supported by FOSSA software composition analysis, which tracks component versions, licenses, and known vulnerabilities. SBOMs are made available to customers on request.

6. Secure Development Practices

Akka's development processes implement the CRA's secure development requirements:

- Threat modelling conducted for all new product features and significant changes
- Code review processes including security-focused review for code handling sensitive operations
- Automated security testing integrated into the CI/CD pipeline
- Dependency scanning and licence compliance via FOSSA
- Infrastructure as Code practices for reproducible, auditable deployments

7. Incident Handling and Notification (Article 14)

Akka maintains a documented incident response procedure aligned with CRA notification requirements. Security incidents involving Akka's products that meet the CRA's severity thresholds are reported to ENISA and relevant CSIRTs within 24 hours (early warning) and 72 hours (incident notification). Customers are notified in parallel in accordance with contractual obligations.

8. End-of-Life and Product Decommissioning

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

Akka provides customers with advance notice of end-of-life dates for product versions and components, giving customers adequate time to migrate. Upon end-of-life, Akka publishes guidance on migration paths and recommends supported versions.

9. Technical Documentation (Annex I, Part II)

Akka maintains technical documentation for its products sufficient to demonstrate compliance with CRA requirements, including:

- Description of the product's intended purpose and cybersecurity features
- Threat modelling and risk assessment documentation
- Vulnerability management processes and policies
- SBOM and dependency documentation
- Testing and assessment records

10. EU Declaration of Conformity

Akka will prepare and maintain an EU Declaration of Conformity for each product within scope of the CRA before placing it on the EU market, once the CRA's conformity assessment requirements become applicable. The Declaration will affirm that the product meets the essential cybersecurity requirements of Annex I of the CRA.

Phased Implementation Status

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

| CRA Obligation | Applicability Date | Status |

|---|---|---|

| Vulnerability reporting to ENISA | December 2026 | Procedures in place |

| Main cybersecurity requirements (Article 13) | December 2027 | 95 controls implemented |

| Notified body conformity assessment (where required) | December 2027 | Preparing |

Supporting Evidence

- ISO/IEC 27001:2022 certification
- SOC 2 Type II report covering security, availability, and confidentiality
- ISO/IEC 27017 cloud security compliance
- FOSSA software composition analysis and SBOM management
- Wiz cloud security posture management
- Coordinated vulnerability disclosure policy at security@akka.io
- Documented SDLC with security review gates
- Published documentation at docs.akka.io and trust.akka.io

Conclusion

AKKA

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

Akka is substantially compliant with the EU Cyber Resilience Act, with 95 of 105 controls fully implemented. The remaining 10 controls are Inactive pending the phased applicability dates under the CRA timeline. Akka's security-by-design development practices, vulnerability management programme, and ISO 27001-certified ISMS provide a strong foundation for full CRA compliance. This attestation is reviewed annually and updated as CRA obligations become applicable.

For further information, please contact compliance@akka.io.

Authorized Signatory:

Michael Nash

Chief Information Security Officer

Akka

580 California Street, #1231

San Francisco, CA 94104

michael.nash@akka.io