**Attestation of Compliance with the Supplier Requirements of the EU Digital Operational Resilience Act (DORA)**

**Issuer:** Akka
**Date:** 2024-04-24
**Subject:** Compliance with Supplier Requirements under EU Regulation 2022/2554 (DORA)

---

## Introduction

Akka is committed to ensuring the operational resilience of its services and products in alignment with the requirements outlined in the **EU Digital Operational Resilience Act (DORA) (Regulation (EU) 2022/2554)**. As a supplier providing critical services to financial entities operating within the European Union, we affirm our adherence to the **supplier-specific obligations** established under the regulation.

---

## Scope of Compliance

This attestation covers Akka's compliance with the following key requirements under **Title III (ICT Third-Party Risk Management)** of DORA:

### 1. Risk Management and Governance

- Akka has implemented an **ICT risk management framework** that aligns with DORA's requirements to ensure the security, availability, and integrity of ICT services provided to financial entities.
- We maintain a **structured governance framework** for managing ICT-related risks, including oversight responsibilities and incident response mechanisms.

### 2. Contractual and Service-Level Compliance

- Our agreements with financial entities include **clear provisions** related to ICT risk management, data security, business continuity, and reporting obligations in accordance with **Article 30 of DORA**.
- Akka commits to **cooperation with financial entities and regulators**, providing necessary information for risk assessments and audits.

### 3. Security and Resilience Measures

- Akka employs **robust cybersecurity controls**, including encryption, multi-factor authentication, and continuous monitoring, to safeguard ICT services.
- Regular **resilience testing** and incident response simulations are conducted to ensure compliance with **Articles 11 and 12 of DORA**.
- Our infrastructure and services comply with **AICPA SOC2, ISO/IEC 27001 and NIST SP 800-53 standards**, ensuring alignment with industry best practices.

### 4. Incident Reporting and Response

- We maintain a structured **incident management program**, ensuring rapid detection, reporting, and mitigation of ICT-related incidents as required under **Article 19 of DORA**.
- Akka provides financial entities with timely notifications of security incidents that may impact their operational resilience.

### 5. Business Continuity and Operational Resilience

- Akka has established **business continuity and disaster recovery plans (BCP/DRP)** to minimize disruptions in ICT services.
- We conduct **regular testing of contingency plans** to ensure the continuity of services critical to financial entities.

### 6. Regulatory Cooperation and Transparency

- Akka **cooperates with competent authorities** in the EU and provides the necessary documentation and reports required for compliance assessments.
- We engage in regular **internal and third-party audits** to ensure continuous alignment with DORA requirements.

## Conclusion

By implementing and maintaining these measures, Akka confirms its compliance with the **supplier obligations** of the **EU Digital Operational Resilience Act (DORA)**. We remain committed to supporting the operational resilience of our financial entity customers and continuously improving our security and risk management practices.

For further details or inquiries regarding Akka's compliance with DORA, please contact **[Insert Contact Information]**.

**Authorized Signatory:**
Michael Nash
CISO/Chief of Staff

Akka

580 California Street, #1231

San Francisco, CA 94104

michael.nash@akka.io