ESMA, the EU, and national regulators launch a Common Supervisory Action targeting CASPs

Deloitte.

Focus: Digital Operational Resilience with Emphasis on Custody Services

This CSA is the **first coordinated European supervisory initiative** focused on the digital operational resilience of CASPs in the crypto custody sector. It provides concrete guidance on which aspects national supervisory authorities **will scrutinize more closely** in the future **and what regulators expect regarding governance, security controls, and custody processes**.
The CSA allows CASPs to identify potential vulnerabilities early and strengthen their audit readiness vis-à-vis regulators and market participants.

Contents

- **Governance Arrangements** – Review of governance structures and organizational measures for crypto custody.
- **Key and Storage Management** – Assessment of key management as well as security and storage mechanisms.
- **Transaction Controls** – Review of controls for transaction processing.
- **Incident Detection & Response** – Review of incident detection, handling, and response.
- **Smart Contract Risks** – Analysis of risks arising from smart contracts.
- **Third-Party Dependencies** – Assessment of external technology and service providers.

Implementation and Timeline

- More than 280 authorized CASPs now fall under the European regulatory framework and are thus at the center of the ongoing convergence of supervisory practices
- Risk-based selection of authorized CASPs by national competent authorities (NCAs).
- Implementation of the CSA in member states from H2 2026 through H1 2027.
- Consolidation of the results by ESMA to promote consistent supervisory practices across the EU.
- Final report to the ESMA-Board of Supervisors in H2 2027.
- Expectation of uniform supervisory practices across the EU, which are likely to significantly shape national reviews in the future.

How Deloitte Can Support

- **CSA Readiness Assessment** to identify regulatory and operational gaps.
- **Mock Regulatory Inspection** based on ESMA audit priorities.
- **Support throughout the CSA**
- **Independent assurance services** covering selected resilience and control domains.
- **Follow-up and remediation** of CSA Findings.

Key audit areas

Potential audit focus areas within the CSA

Governance Arrangements

Responsibilities and expertise for crypto-asset custody and ICT at the management level, Three Lines of Defence, consideration of DLT risks within the ICT risk strategy and ICT risk management, outsourcing governance.

Key and Storage Management

Secure generation, rotation, and destruction of cryptographic keys; cryptographic parameters and algorithms used such as curves and signature schemes, MPC architecture, HSM storage, backup and recovery procedures, access and administration concepts, particularly quorum requirements, and physical security mechanisms.

Transaction Controls

Whitelisting, limits, approval concepts and workflows, audit trails, protection against address poisoning and blind signing, reconciliation of on-chain holdings against book records, evidence of segregation between client and proprietary assets pursuant to Articles 70 and 75 MiCAR, anti-money laundering controls and sanctions management.

Incident Detection & Response

Logging and monitoring, severity classification, reporting channels and deadlines pursuant to DORA Articles 17–19, crisis and emergency exercises, and post-incident reviews.

Smart Contract Risks

Audits prior to deployment, upgradeability and administrative keys, bridge, staking and delegation risks, and handling of chain reorganisations and forks.

Third-Party Dependencies

Sub-service providers and sub-custodians, wallet technology providers, cloud and node providers, DORA-compliant contractual clauses, the register of information, concentration risks and exit strategies.

Your Contacts

ALIREZA SIADAT
PARTNER

Mobile: +49 176 747 23 068
Email: asiadat@deloitte.de

ALEXEY WEIZMANN
DIRECTOR

Mobile: +49 151 580 72 773
Email: aweizmann@deloitte.de

NICO HASS
DIRECTOR

Mobile: +49 151 580 05318
Email: nihass@deloitte.de