

ECB CROE — Cyber Resilience Oversight Expectations for Financial Market Infrastructures



ECB CROE sets supervisory expectations to strengthen

What it is Cyber resilience, risk management, and incident response of systemically important FMIs.

ECB CROE — Cyber Resilience Oversight Expectations for Financial Market Infrastructures is a supervisory framework that establishes standardized expectations for the cyber resilience of financial market infrastructures (FMIs), supporting the stability and security of critical financial services. This framework aims to strengthen organizations' ability to prevent, respond to, and recover from cyber incidents that could impact the wider financial system.

Published by the European Central Bank (ECB), ECB CROE applies to systemically important FMIs within the Eurozone, including payment systems, central securities depositories, and central counterparties. It focuses on areas such as cybersecurity controls, risk management, incident response, and operational resilience, aligning with global principles from organizations like CPMI-IOSCO.

At a glance

PUBLISHER European Central Bank (ECB)	TYPE Guidance	VERSION CROE Framework
EFFECTIVE 2019	DOMAIN Operational Resilience	FAMILY Other
REGION Euro area	INDUSTRY Financial Services	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source:
https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

Why it matters

- **Strengthen cybersecurity governance** Support effective leadership oversight and security policy enforcement across all aspects of financial market infrastructure operations.
- **Enhance risk management practices** Enable comprehensive identification, assessment, and mitigation of cyber risks to minimize potential disruption to financial services.
- **Promote regulatory alignment** Demonstrate compliance with ECB and international standards, facilitating consistent supervisory engagement and stakeholder confidence.
- **Improve incident response capabilities** Enhance preparedness to detect, manage, and recover from cyber incidents, reducing impact and supporting continuity of operations.

How SmartSuite supports ECB CROE

CROE Expectation Mapping

Map CROE expectations to controls, owners, and evidence sources.

Test Scheduling and Remediation Tracking

Schedule tests, capture results, and track remediation through closure.

Situational Awareness Evidence Hub

Track monitoring coverage, threat intelligence inputs, and detection validation proof.

Incident Response and Recovery Workflows

Run incidents and recovery tasks with full documentation and improvement actions.

Third-Party and Dependency Oversight

Manage provider risk, monitoring, and exit planning evidence.

Executive and Oversight Reporting

Report readiness, gaps, and maturity progression for governance stakeholders.

Common framework mappings

EU DORA

ISO 22301

ISO 27001:2022

ISO 27002:2022

NIST CSF 2.0

NIST 800-53 Rev.5

SWIFT CSCF

Official resources

ECB Cyber Resilience Oversight Expectations Document

Defines the cyber resilience expectations for financial market infrastructures as published by ECB.

ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

Frequently asked questions

What is ECB CROE used for?

ECB CROE is used to establish standardized expectations for the cyber resilience of systemically important financial market infrastructures (FMIs) within the Eurozone. The framework ensures these organizations can protect, detect, respond to, and recover from cyber incidents, thus contributing to the stability of the broader financial system.

Is ECB CROE mandatory or certifiable?

ECB CROE is not a certifiable standard, but it is a supervisory expectation issued by the European Central Bank for critical FMIs. Compliance is required for FMIs overseen by the ECB, and adherence is reviewed through regulatory oversight activities rather than a formal certification process.

Which organizations does ECB CROE apply to?

ECB CROE applies to systemically important FMIs operating within the Eurozone, such as payment systems, central securities depositories, and central counterparties. Organizations are expected to align with CROE if they are designated as critical to financial market infrastructure stability.

What are the key domains or control areas in ECB CROE?

The framework is structured around operational resilience domains, including governance, identification, protection, detection, response, and recovery. Each domain contains requirements for risk management processes, security controls, incident response, and continuous improvement.

How do organizations implement ECB CROE requirements?

Implementation involves assessing current resilience practices against CROE's expectations, conducting risk assessments, updating security controls, and refining incident response and recovery plans. Organizations must document compliance activities, conduct regular reviews, and ensure continuous improvement of cyber resilience capabilities.

How does ECB CROE align with other cybersecurity frameworks?

ECB CROE is informed by global benchmarks such as CPMI-IOSCO guidance and other regulatory and industry standards. Alignment allows organizations to integrate CROE requirements into existing compliance programs and leverage synergies with frameworks like ISO 27001 or NIST CSF.

What are the ongoing compliance and maintenance requirements for ECB CROE?

Organizations must regularly review and update resilience controls, conduct incident response exercises, and monitor the effectiveness of risk mitigation measures. Ongoing oversight, audit trails, and continuous improvement are essential to demonstrate continued alignment with ECB CROE expectations.

How would SmartSuite support ECB CROE?

SmartSuite enables organizations to manage ECB CROE by centralizing risk tracking, mapping and tracking control implementation, and organizing supporting evidence for compliance. The platform offers incident and remediation workflows, real-time dashboards for audit readiness, and reporting tools to support documentation and oversight of operational resilience activities.

License included / downloadable: Yes The ECB Cyber Resilience Oversight Expectations framework is publicly available through the European Central Bank.

Full framework page and mappings: smartsuite.com/frameworks/ecb-croe-cyber-resilience-oversight-expectations-for-financial-market-infrastructures