SmartSuite

Framework / Operational Resilience / Other

ECB CROE — Cyber Resilience Oversight Expectations for Financial Market Infrastructures

The ECB's Cyber Resilience Oversight Expectations set evolving, advancing and innovating levels across eight categories for payment systems, T2S and other FMIs.



What it is

The Cyber Resilience Oversight Expectations (CROE) are the European Central Bank's detailed expectations for how financial market infrastructures (FMIs) operationalize the CPMI-IOSCO Guidance on cyber resilience, set at three levels (evolving, advancing and innovating) across eight categories. Eurosystem overseers apply them to all payment systems and to TARGET2-Securities (T2S). The ECB published the document in December 2018.

The ECB's Governing Council adopted the CROE, and Eurosystem overseers use it to assess FMIs. It applies directly to payment systems and T2S. For central securities depositories, securities settlement systems and central counterparties, oversight sits mostly with national central banks and authorities, which may choose to use the CROE under their own laws.

At a glance

PUBLISHER
European Central Bank (ECB), Eurosystem oversight

TYPE
Guidance

VERSION
Cyber resilience oversight expectations for financial market infrastructures, December 2018

EFFECTIVE
December 2018

DOMAIN
Operational Resilience

FAMILY
Other

REGION
Euro area

INDUSTRY
Financial Services

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html

Why it matters

- **A clear benchmark for overseers** The CROE gives overseers the expectations they use to assess an FMI and a basis for a meaningful discussion with it (section 1.2).
- **Three levels that show progress** Evolving, advancing and innovating let an FMI measure where it stands and set priorities for improvement (section 1.4.1).
- **Proportionate expectations** Retail payment systems are expected to reach evolving as a minimum, while systemically important payment systems and T2S are expected to reach advancing (section 1.4.2).
- **Flexibility with accountability** An FMI that does not meet an expectation explains how it meets the underlying objective, under the meet-or-explain principle (section 1.4.2).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ECB CROE

Expectation Library by Level

Hold the expectations for each chapter and level, with the FMI's target level, owner and evidence (sections 1.4 and 2).

Board and Senior Executive Accountability

Record the board-approved strategy and framework, the senior executive role and the review calendar (sections 2.1.2.1 and 2.1.2.2 and Annex 3).

Critical Function and Asset Register

Link critical functions, information assets, service providers and interconnections to the identification and protection expectations (sections 2.2 and 2.3).

Incident and Recovery Workflow

Run incident management, recovery objectives, data integrity checks, communication and forensic readiness as tracked procedures (section 2.5).

Testing and Threat Intelligence Plan

Schedule vulnerability assessments, scenario-based tests and penetration tests, and log threat intelligence and information sharing (sections 2.6 and 2.7).

Meet-or-Explain Reporting

Record each expectation not met, the explanation of how its objective is still met, and the action plan, for discussion with the overseer (section 1.4.2).

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 the ECB CROE?

The Cyber Resilience Oversight Expectations are the ECB's detailed expectations for how financial market infrastructures put the CPMI-IOSCO cyber resilience Guidance into practice. They set three levels of expectation and are used by Eurosystem overseers to assess FMIs (sections 1.2 and 1.4).

What are the three levels of expectation?

Evolving means essential capabilities are established and sustained. Advancing adds more advanced, integrated tools that manage cyber risk proactively. Innovating adds enhanced capabilities and proactive collaboration with external stakeholders (section 1.4.1).

Which FMIs must reach which level?

All prominently important and other retail payment systems are expected to reach and maintain evolving as a minimum. Systemically important payment systems and T2S are expected to reach and maintain advancing (section 1.4.2). Other authorities decide the level for CSDs, CCPs and trade repositories.

Is the CROE a checklist?

No. The document says it should not be considered a checklist of measures to be strictly complied with. FMIs that do not meet an expectation explain how they meet its underlying objective, under the meet-or-explain principle (section 1.4.2).

What does the CROE cover?

Five risk management categories, which are governance, identification, protection, detection, and response and recovery, and three components, which are testing, situational awareness, and learning and evolving (section 1.5 and chapter 2).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

License included / downloadable: Yes The CROE document is published free by the European Central Bank and is included with the platform for reference.

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

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.