



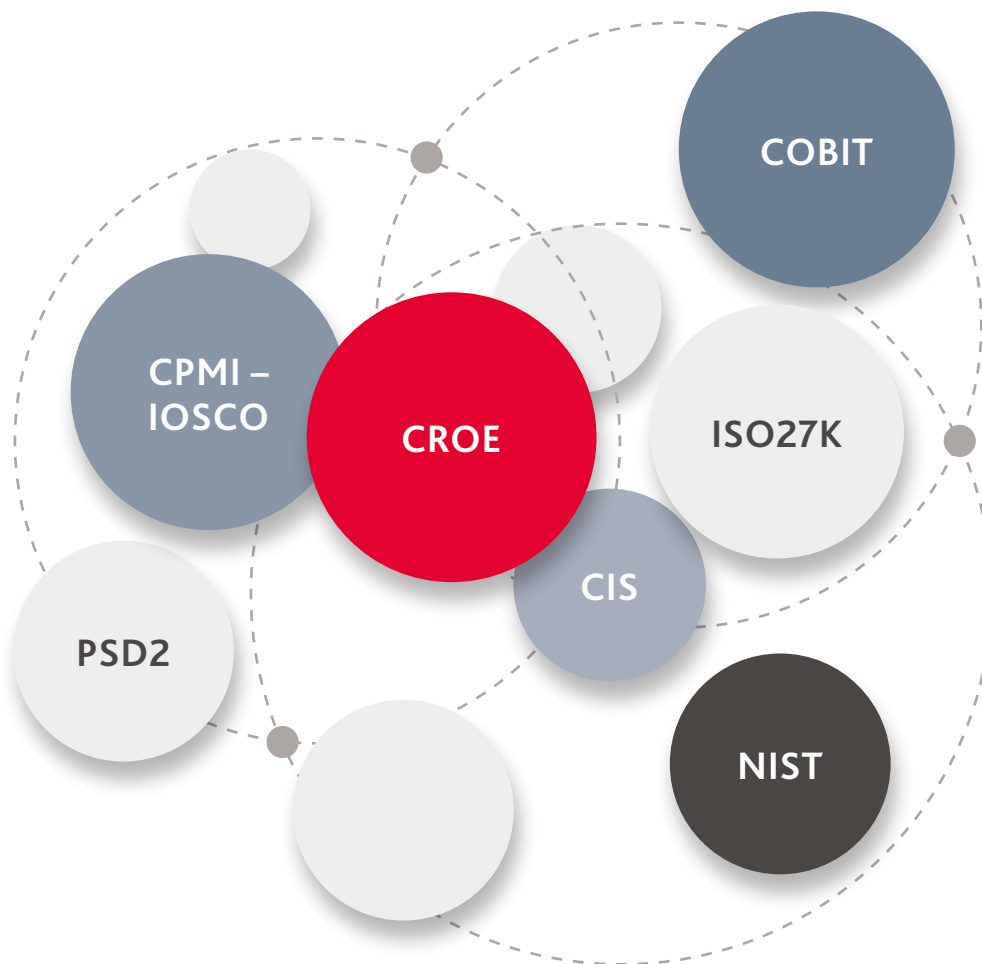
BDO RISK ADVISORY SERVICES

CYBER RESILIENCE

REGULATORY COMPLIANCE

CROE:

A MUCH NEEDED SIMPLIFICATION OF THE CYBER REGULATORY LANDSCAPE FOR FINANCIAL INSTITUTIONS?



Cyber threats have emerged as a systematic concern for the financial sector, and especially for the Financial Market Infrastructures (FMI's), because of their unique role and characteristics. In this context, the ECB has imposed the financial sector to comply with multiple cyber resilience regulations. The sector has made extensive efforts to comply with these expectations by implementing one or more cyber security frameworks (NIS, ISO27001, COBIT ...). Yet it remained difficult to properly comply with the expectations of the regulator due to a lack of operational and detailed methodology. The ECB has recognised this issue and has

published the Cyber Resilience Oversight Expectations (CROE) as a solution. This methodology sets out clear criteria for the FMI's to work with, establishing a detailed basis for discussion with the regulator. The great news is that the ECB has used existing international cyber resilience frameworks as input for developing the CROE, meaning that the efforts to comply with one of these standards can be built upon to accelerate compliance with CROE.

In this brochure we would like to give you some initial insights in the CROE and show you how it can be used as an opportunity to streamline your current cyber resilience landscape.

CYBER RESILIENCE REGULATORY EVOLUTION

ADDRESSING CYBER RISKS AS A SOURCE OF SYSTEMIC RISK TO THE FINANCIAL SYSTEM

Regulatory Background

With the coming into force of a comprehensive new package of EU and national level cyber security regulations, certain categories of businesses in the financial services industry are required to ensure compliance with the new rules and to implement an adequate and robust cyber security framework.

In December 2018, the European Central Bank (ECB) published the **Cyber Resilience Oversight Expectations (CROE)** defining the Eurosystem's expectations in terms of cyber resilience. The CROE is applicable to both large value and retail payment systems, and generally to all the Financial Market Infrastructures (FMIs).

The CROE provides overseers with a framework to assess the cyber resilience of systems under their responsibility, and enables the FMIs to enhance cyber resilience. The FMIs are defined by the NIS Directive as:

- Operators of trading venues (including regulated markets, and both multilateral and organized trading facilities);
- Central counterparties, which are defined as "a legal person that interposes itself between the counterparties to the contracts traded on one or more financial markets, becoming the buyer to every seller and the seller to every buyer".

With the ECB as the lead overseer, The Eurosystem conducts the oversight on a cooperative basis with the active involvement of all national central banks in the Eurosystem. The **National Bank of Belgium (NBB)** is responsible for the oversight of the Belgian domestic retail payment system and uses the CROE for assessing its cyber resilience.

CROE purpose

The **Cyber Resilience Oversight Expectations (CROE)** serves three key purposes:



It provides supervisory/oversight authorities with clear expectations to assess the FMIs actors under their responsibility and their respective cyber resilience maturity levels;



It gives the FMIs detailed steps on how to operationalise the given CROE guidance, ensuring that they are able to foster improvements and enhance their cyber resilience;



It serves as the basis for a common understanding and a detailed and meaningful discussion between the FMIs and their respective overseers, like the NBB.

The purpose of the CROE is to primarily assist the supervisory/oversight authorities in the review of compliance with the guidance as part of their oversight function, so - in essence - it is akin to an assessment framework.

However, the CROE is not designed as or intended to be a formal cybersecurity framework, but a practical tool to assist authorities in assessing the cybersecurity frameworks used by organisations whose oversight they are responsible for.

Unlike other sets of oversight standards, the CROE enables overseers to determine for each of the eight domains covered which of the three maturity levels proposed (Evolving, Advancing, Innovating) must be achieved, according to the risk profiles and specific activities involved.



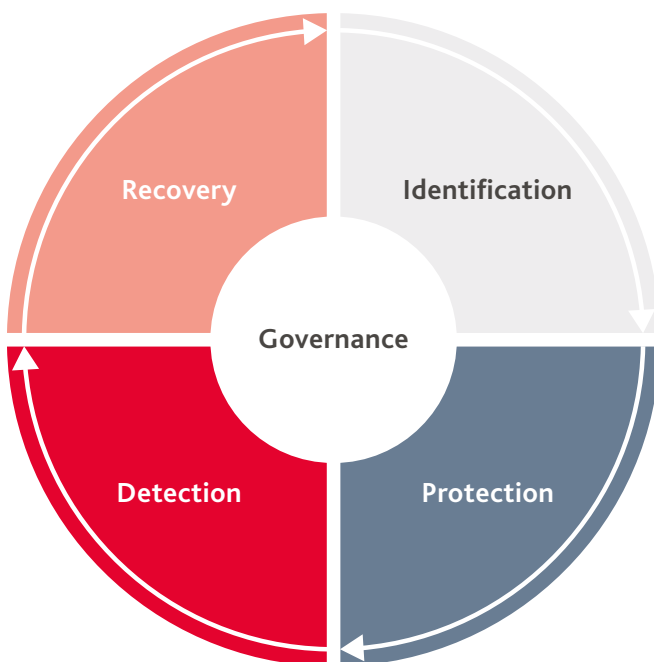
CYBER RESILIENCE OVERSIGHT EXPECTATIONS (CROE)

COMPONENTS OF THE FRAMEWORK

Domains covered by CROE

The CROE is drafted in a technological, operational and jurisdictional agnostic manner and covers eight domains that should be addressed across an FMI actor's cyber resilience framework:

- Five primary risk management pillars: **Governance, Identification, Protection, Detection, Response and Recovery**;
- Three overarching components: **Testing, Situational Awareness, Learning and Evolving**.



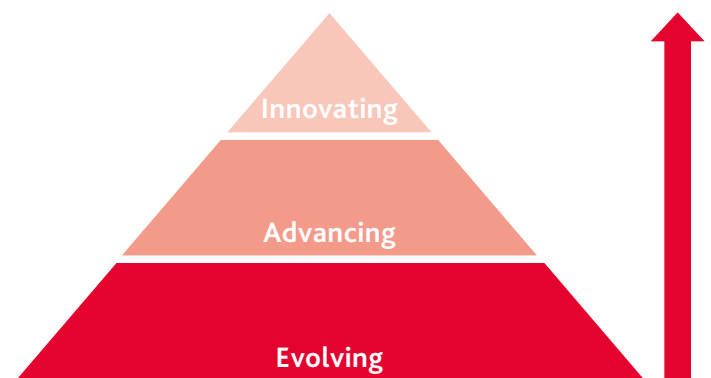
Source: CROE framework, European Central Bank 2018

These are translated into sections of CROE that further detail the overarching expectation and the qualitative features that must be fulfilled by the FMI actors to meet each expectation level.

While the CROE has been developed to provide FMIs with detailed and specific expectations, it also allows for a degree of flexibility when dealing with a heterogeneous set of FMI actors in size, volume and value of transactions, as well as their role within the financial system. Therefore, the role and the interpretation of the supervisory/oversight authority (like NBB) in applying this flexibility and judgement is very important.

Levels of CROE expectation

The **Cyber Resilience Oversight Expectations (CROE)** sets out three levels of expectation (also referred to as 'maturity levels'). They provide both the supervisory/oversight authorities and FMI actors with a benchmark against which they can evaluate the FMI's current level of cyber resilience, measure its progress and establish priority areas for improvement.



The three levels of expectation are defined below.

Evolving: Essential capabilities are established, evolve and are sustained across the FMI actor's organisation to identify, manage and mitigate cyber risks, in alignment with the cyber resilience strategy and framework approved by the Board. Performance of practices is monitored and managed.

Advancing: In addition to meeting the evolving level's requirements, practices at this level involve implementing more advanced tools (like advanced technology and risk management tools) that are integrated across the FMI actor's business lines and have been improved over time to proactively manage cyber risks posed to the FMI actor.

Innovating: In addition to meeting the evolving and advancing levels' requirements, capabilities across the FMI actor are enhanced as needed within the rapidly evolving cyber threat landscape, in order to strengthen the FMI actor's cyber resilience and its ecosystem and by proactively collaborating with its external stakeholders. This level involves driving innovation in people, processes and technology for the FMI actor and the wider ecosystem to manage cyber risks and enhance cyber resilience. This may call for new controls and tools to be developed or new information-sharing groups to be created.

WHAT ORGANISATIONS ARE SUBJECT TO CROE?

A FRAMEWORK USED BY NBB FOR ASSESSING CYBER RESILIENCE OF BELGIAN FINANCIAL ACTORS

Are you a subject of the CROE?

The CROE will be applied by the Eurosystem (i.e. the Eurozone central banks) for the oversight of all payment systems and T2S. More precisely, ECB intends that CROE will be applied by the Eurosystem to:

- Systemically Important Payment Systems (SIPS);
- Prominently Important Retail Payment Systems (PIRPS);
- Other Retail Payment Systems (ORPS);
- TARGET2-Securities System (T2S).

National Central Banks, operating under national law, often in conjunction with other competent authorities may opt-in to use the CROE for any and all 'other' FMIs, as for example clearing and settlement systems:

- Central Securities Depositors (CSDs);
- Central Counterparties (CCPs), etc.

We anticipate CROE will become, as has been already the case in other ECB rulemaking exercised by way of non-binding guidance, more widely adopted by the core Eurozone Member States, in particular by those with significant FMIs operating within their jurisdiction.

FMI Actor	Applicability of CROE Expectations
PIRPS ORPS	Reach and maintain the evolving level, as a minimum, with active steps to be taken over time by the actor to attain an advancing level, where deemed appropriate.
SIPS T2S	Reach and maintain the advancing level, with active steps to be taken over time by the actor to attain an innovating level, where deemed appropriate.
Others	At the discretion and judgement of the supervisory/oversight authority.

The supervisory/oversight authorities (e.g. NBB) will judge whether the FMI actor is meeting – as applicable – the **evolving, advancing or innovating** CROE levels.

This judgement is driven by a number of considerations such as the local laws and regulations governing the FMI actor; the NBB's broader historic knowledge of the FMI; the FMI's size, criticality and business model; and the ongoing discussions between NBB and the FMI.

FMI actors shall reach CROE levels of expectation across all categories: **Governance, Identification, Protection, Detection, Response and Recovery, Testing, Situational Awareness, Learning and Evolving.**

Once they reach and maintain their prescribed levels of expectation, they should evolve and improve by taking relevant steps to reach the higher levels, where appropriate and in line with their business specifics. This process of evolution and improvement should occur through discussions between the supervisory/oversight authorities and the FMI actor, and over a period of time.

Meet or explain principle

The three levels of expectation are intended to allow the FMI actor to build and improve its capabilities in a multilayered way over a longer period of time, with each level of expectation building additional mutually reinforcing good practices on top of each other.

Therefore, the FMI actor should review the CROE in detail, understand it and consider how to implement the expectations contained within it, giving due consideration to how best to build, improve and use its people, processes and technologies for cyber resilience.

The CROE frequently uses the term capabilities, which refers to the "people, processes and technologies the FMI actor uses to identify, mitigate and manage its cyber risks and to support its objectives."

As FMI actors implement the CROE expectations, it is acknowledged that at times they will do so in different ways. In cases where the FMI actor does not meet the prescribed expectation, it should provide an explanation as to how it meets the objective of the underlying expectation.

The **meet or explain principle** provides flexibility for the approach used to enhance cyber resilience capabilities, given that FMI actors are heterogeneous and they differ in size, in organisational and operating structure, business model and infrastructure set-up.

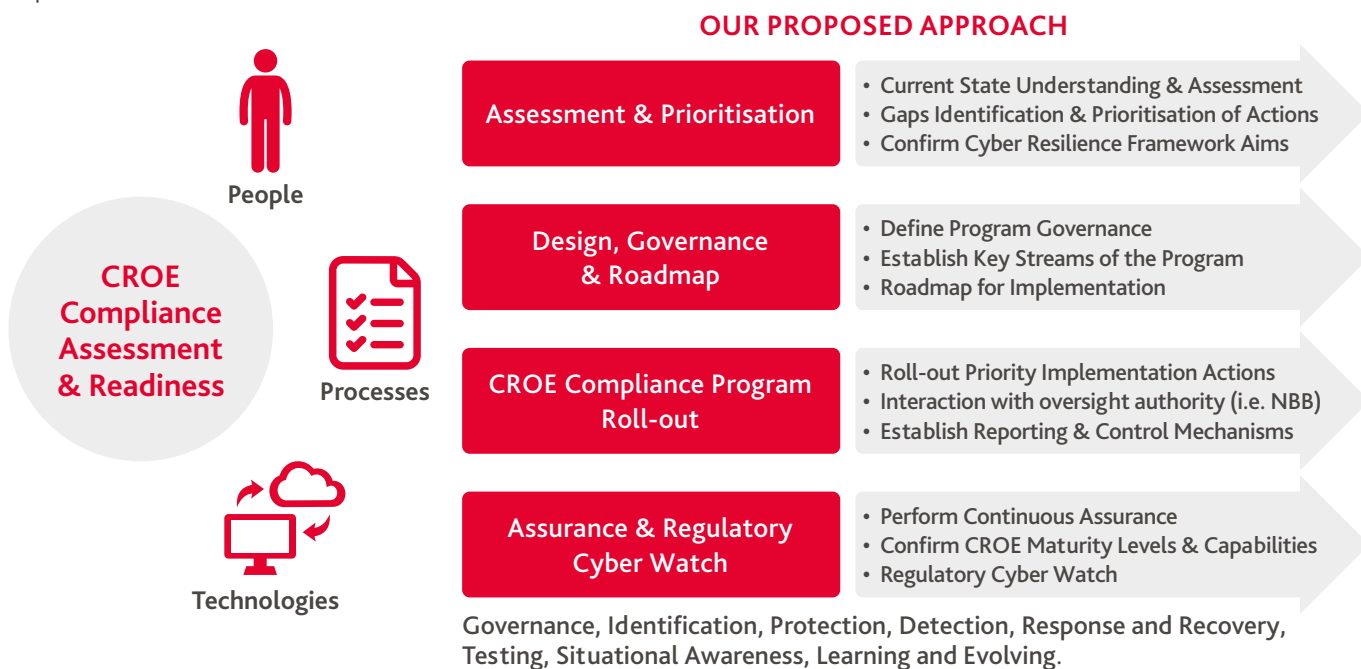
AVOID TYPICAL PITFALLS IN COMPLYING WITH CROE

Common errors made by FMI actors:

- **Insufficient understanding** of the CROE framework
- **Lack of a well-managed** internal cyber resilience program for achieving CROE compliance
- Insufficient identification and/or ineffective management of **cyber security risks**
- **Inadequate testing** of cyber security control effectiveness
- **Weak governance** of cyber resilience efforts
- **Incorrect self-assessment** on achieving a level of CROE expectation: **evolving, advancing, innovating**
- Insufficient **identification of IT assets** and their cyber security protection needs
- Inadequate cyber incident **detection and/or response capabilities**

HOW CAN BDO HELP YOU?

BDO has the necessary expertise and track record in advising key FMI actors to take appropriate cyber resilience measures for CROE compliance. BDO offers you the information, the practical approach and solutions for dealing with the NBB and ECB supervisory requirements under the CROE framework.





Interested? Get in touch with:

KOEN CLAESSENS
Partner Risk Advisory Services
E-mail: koen.claessens@bdo.be
Tel.: +32 (0)497 51 53 83

STEVEN CAUWENBERGHS
Partner Risk Advisory Services
E-mail: steven.cauwenberghs@bdo.be
Tel.: +32 (0)497 05 12 23

SAM NELEN
Manager Risk Advisory Services
E-mail: sam.nelen@bdo.be
Tel.: +32 (0) 486 91 12 20

► Follow us    
► www.bdo.be