CROE
Cyber Resilience Oversight Expectations

Guest speaker:
Dan Cimpean - General director, CERT-RO

CROE center of expertise:
Sam Nelen - BDO BE
Steven Cauwenberghs - BDO BE
Content

- Cyber Resilience framework by the ECB, December 2018
  - Regulatory trends, CROE framework

- CROE compliance: a pragmatic approach
  - Practical example

- Inspection by regulators
  - Main findings

- Key success factors
Financial services firms are 300 times as likely as other companies to be targeted by a cyberattack.

Source: report by the Boston Consulting Group
Out of the total number of national-level cyber incidents: 12% impacted the banking sector 0.5% impacted the financial market infrastructures.
THE CYBER TRENDS
Financial sector - what regulators and cyber competent authorities try to do?

Try to handle all these at once...

A structured, focused and coherent approach is needed...
THE REGULATORY TRENDS
The approach of the ECB

Pillar 1: FMI Readiness
- CROE
- TIBER-EU

Pillar 2: Sector Resilience
- Interconnected
- Info-sharing network

Pillar 3: Strategic Regulator - Industry engagement
- Euro Cyber Resilience Board for pan-European FMIs (ECRB)
THE REGULATORY TRENDS
The approach of the ECB

- CPMI-IOSCO Guidance on Cyber Resilience for FMIs
- European Red Team Testing Framework (TIBER-EU)
- Euro Cyber Resilience Board for pan-European FMIs (ECRB)

2016
- Eurosysten cyber resilience strategy for FMIs

2017
- Cyber Resilience Oversight Expectations (CROE)

2018
- Inspections, readiness, cyber resilience actions

ongoing
CROE FRAMEWORK
The specifics

i. It provides oversight authorities with clear expectations to assess the FMIs actors

ii. It gives FMIs detailed steps on how to operationalise the CROE guidance

iii. It serves as the basis for a common understanding and a detailed and meaningful discussion between FMIs and their oversight authorities
CROE FRAMEWORK
Level of expectations - maturity levels

CROE maturity levels:
- Innovating
- Advancing
- Evolving

Expectations by type of FMI:
- Proportionality principle
- Minimum requirements

Clear guidelines per level:
- Comply or explain

Adapt to a changing cyber environment:
- Continuously evolve on the cyber maturity scale

Governance
- Recovery
- Identification
- Detection
- Protection

Learning and evolving
Situation awareness
Testing
CROE FRAMEWORK
Evolving vs Advancing vs Innovating level

Evolving
- Essential capabilities to identify, manage and mitigate cyber risks
- In alignment with the Board-approved cyber resilience strategy and framework
- Performance of practices is monitored and managed

Advancing also requires
- More advanced implementations (e.g. advanced technology and risk management tools)
- Proactively manage cyber risks

Innovating also requires
- Proactively collaborating with external stakeholders
- Driving innovation in people, processes and technology
CROE FRAMEWORK
Applicability

As defined by the ECB

- SIPS = Systematically Important Payment System
- PIRPS = Prominently Important Retail Payment System
- ORPS = Other Retail Payment System
- CCP = Central Clearing Party
- CSD = Central Securities Depository
- TR = Trade Repository
- NCB = National Central Bank

* Banks and other FIs do not directly fall under the CROE, however this still remains a very good practice framework acknowledged across Europe, and might even become acknowledged worldwide.
# CROE FRAMEWORK

## Market players

<table>
<thead>
<tr>
<th>Advancing</th>
<th>Evolving</th>
<th>Discretion of NCBs</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIPS</td>
<td>PIRPS</td>
<td>CCP</td>
</tr>
<tr>
<td>ORPS</td>
<td></td>
<td>CSD</td>
</tr>
<tr>
<td>Trade Repositories</td>
<td>Card Payment Schemes</td>
<td>Payment systems</td>
</tr>
</tbody>
</table>

- **target**
- **nexi**
- **ice**
- **DTCC**
- **AMERICAN EXPRESS**
- **giropay**
- **EBA CLEARING**
- **iberpay**
- **iccrea Banca**
- **LCH**
- **Monte Titoli**
- **REGIS-TR**
- **UP**
- **PSA**
- **Worldline**
- **OLME**
- **cleanstream**
- **DEUTSCHE BÖRSE GROUP**
- **SIX**
- **UnionPay International**
- **paysquare**
- **mastercard**
- **BHE CLEARING**
- **Nasdaq**
- **CME Group**
- **VISA**
- **DISCOVER NETWORK**
- **CCP**
- **INTERBOLSAY**
- **Bloomberg**
- **DISCOVER NETWORK**
INSPECTION BY REGULATORS

Timeline

Publication of CROE

Dec 2018

National Bank of Belgium uses CROE framework in its oversight activities

2019

National Bank of Belgium uses CROE framework in its oversight activities

WHO IS NEXT?

The ECB wins Central Banking Award for its CROE framework

Nov 2019

Self-assessment exercise on request of the oversight function

The World Bank adopts CROE

Feb 2020

Bank of France uses CROE framework in its oversight activities

2020

Self-assessment exercise on request of the oversight function

The World Bank

WHO IS NEXT?

The ECB wins Central Banking Award for its CROE framework
### INSPECTION BY REGULATORS

**Main findings**

<table>
<thead>
<tr>
<th>Lack of testing of the effectiveness of the cyber strategy</th>
<th>Lack of awareness and training</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unclear overall cyber governance and/or strategy</td>
<td>Insufficiently developed IT security detection capabilities</td>
</tr>
<tr>
<td>Insufficient identification and ineffective management of IT security risks</td>
<td>Insufficiently developed IT security response capabilities</td>
</tr>
<tr>
<td>Insufficient segregation and protection of administration access</td>
<td>Weaknesses in logical access management</td>
</tr>
</tbody>
</table>
BEST PRACTICES
CROE Compliance Assessment & Readiness: a pragmatic approach

Key project steps

- Determine the required cyber resilience level
- Perform a GAP analysis between the existing cyber program and CROE
- Make a thorough risk assessment of the cyber exposure
- Establish a feasible roadmap and prioritize actions
- CROE Compliance Program Roll-out

Phase 1

Determine the required cyber resilience level

Phase 2

Perform a GAP analysis between the existing cyber program and CROE

Make a thorough risk assessment of the cyber exposure

Establish a feasible roadmap and prioritize actions

Phase 3

Establish a feasible roadmap and prioritize actions

Leverage upon the experience, governance and results of the existing cyber program and all other cyber projects and actions of company ABC, we do not start from scratch!

Always consider

- The company’s strategy
- Regulations & Frameworks
- Threat & Risk Landscape
- Risk Management & Appetite
- Assets & Sourcing
- Experienced professionals
BEST PRACTICES
CROE Compliance Assessment & Readiness: a pragmatic approach

Phase 1
Readiness assessment
- Perform a self-assessment
- Build up initial supporting documentation and formally submit the file to the overseer
- Align existing cyber projects and programs

Phase 2
Establish Roadmap
- Analyze the final report received from the overseer
- Prioritize actions and document a roadmap that is accepted by all stakeholders
- Assign responsibilities

Phase 3
Implementation
- Set-up a strong governance structure across all cyber related area’s
- Follow-up and implement all actions in the required timeframe
- Comply or explain principle

Full compliance with CROE framework
- Ongoing effort
- Evolving Advancing Innovating

Governance
- Recovery
- Detection
- Protection
- Testing
- Situational awareness
**Phase 1: Readiness Assessment**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Requirement</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario-based testing</td>
<td>The FMI should conduct scenario-based tests that cover breaches affecting multiple portions of the FM’s ecosystem in order to identify and analyse potential complexities and interdependencies both at business and operational level which should be taken into account in the FMI’s cyber resilience framework.</td>
<td>Compliant</td>
</tr>
<tr>
<td></td>
<td>The FMI should collaborate with the ecosystem to develop cybersecurity incident scenarios involving significant financial loss and use them for stress tests to better understand potential spillovers and contagion risk to the ecosystem. The FMI should use such stress tests to further improve its cyber resilience posture, which contributes to the improvement of the resilience of the ecosystem as a whole.</td>
<td>Partially compliant</td>
</tr>
<tr>
<td>Red-teaming tests</td>
<td>In addition to periodic independent, external red-team exercises, the FMI should develop an internal red-team capability, with the appropriate methodologies, sophisticated tools and appropriately skilled personnel. The internal red-team test should regularly conduct red-team exercises and engage with the internal blue team, to transmit its findings and make improvements to the FMI’s cyber resilience posture.</td>
<td>Not compliant</td>
</tr>
</tbody>
</table>

- The FMI’s cyber resilience level determines the applicable requirements of the CROE
- Alignment of existing cyber program with the requirements is essential to minimize efforts and related investments
- Documentation is key, it is not just completing a checklist!
- Don’t wait for the final report of the overseer, but start listing the preliminary actions already
**CROE FRAMEWORK**  
Based on known standards

Leverage the existing cyber program to minimize the efforts required by the company

<table>
<thead>
<tr>
<th>Topic</th>
<th>CROE</th>
<th>ISO27001</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Governance</td>
<td>Cyber resilience strategy and framework</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Role of the Board and senior management</td>
<td></td>
</tr>
<tr>
<td>2. Identification</td>
<td>Business processes and information assets</td>
<td></td>
</tr>
<tr>
<td>3. Protection</td>
<td>Protection of processes and assets</td>
<td></td>
</tr>
<tr>
<td></td>
<td>People management</td>
<td></td>
</tr>
<tr>
<td>4. Detection</td>
<td>Detect cyber incidents</td>
<td></td>
</tr>
<tr>
<td>5. Response and recovery</td>
<td>Cyber resilience incident management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data integrity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communication and collaboration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Forensic readiness</td>
<td></td>
</tr>
<tr>
<td>6. Testing</td>
<td>Vulnerability assessments</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scenario-based testing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Penetration tests</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Red team testing</td>
<td></td>
</tr>
<tr>
<td>7. Situational awareness</td>
<td>Cyber threat intelligence</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information sharing</td>
<td></td>
</tr>
<tr>
<td>8. Learning and evolving</td>
<td>Cyber threat intelligence</td>
<td></td>
</tr>
</tbody>
</table>
BEST PRACTICES
CROE Compliance Assessment & Readiness: a pragmatic approach

Phase 2: Establish roadmap

Step 1
Risk Analysis
- Current state understanding & assessment of the NCB report findings & implications
- Translate NCB findings in actionable terms, by re-confirming NCB gaps and findings with stakeholders/ risk owners

Step 2
Root Cause Identification
- Confirm the key risks noted
- Deep-dive into the risks raised by NCB in order to accurately assess their root cause (specific, transversal, Group-wide, etc.)
- Touch-point with NCB

Step 3
Clustering of Root Causes
- Clustering of root causes
- Identify common topics and synergies to help addressing the risks
- Define strategy for risk mitigation actions (exhaustive, priority-based, minimal compliance, etc.)

Step 4
Establish roadmap
- Inventory of ongoing actions and improvements
- Risk-based prioritization of mitigation actions
- Confirm the building blocks for the roadmap
- Touch-point with NCB
Phase 3: Implementation

- Periodical interaction with the overseer is required to keep them informed of the roll-out process
- Strong governance structure is required to streamline all actions across the entire FMI

Roadmap for Implementation

Implementation of key improvement actions to mitigate risks and address NCB findings
KEY SUCCES FACTORS
CROE compliance

Leverage existing cyber program to minimize the efforts required by the company.

Build up sufficient documentation to support cyber resilience level to convince the regulator.

Understand the expectations of the regulator and use professional judgement to determine the roadmap to full compliance.

Ongoing effort to increase cyber resilience level in function of changing technologies and business, this is not a one off exercise.

Don’t hesitate to ask for support from your regulator or from experts.
ABOUT BDO

BDO Global
As of November 2019

- Global revenue: 9.6 Bn USD
- Countries and territories: 167
- People: 88,000+

BDO Belgium
As of 2019

- Revenue: 104.2 Mn EUR
- Audit & Assurance: 25%

Our people

- Professional staff: 559
- Partners: 743
- Support staff: 88
- 96