RegCORE Client Alert

Revisiting the European Central Bank's cyber-resilience oversight expectations (CROE)

December 2021

European Central Bank's cyber-resilience

Revisiting the European Central Bank's cyber-resilience oversight expectations (CROE)

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas
@pwc.com

Contact RegCORE Team
de_regcore@pwc.com

A functioning real economy requires the financial system to perform a range of key economic functions reliably. These include payment services, securities trading, settlement services and deposit taking, among others. These processes have become increasingly digitalised, creating new and important interdependencies often with a limited number of service providers. The financial system has come to rely critically on robust information and communications technology (**ICT**) infrastructures and the confidentiality, integrity and availability of data and systems. Consequently, critical economic functions can be disrupted through cyberattacks and other incidents that affect the information systems and data of financial institutions and financial market infrastructures. Cyber-attacks can turn into systemic crisis when trust in the financial system is eroded[1].

The European Central Bank (**ECB**), acting in its central banking and financial stability role as opposed to its financial regulatory and supervisory role at the head of the Banking Union's Single Supervisory Mechanism (**SSM**) took the first (welcome) steps into improving cyber-resilience standards across the financial services sector[2].

During December 2018, the ECB published its Resilience Oversight Expectations (the **CROE**) for financial market infrastructures (**FMI**)[3]. CROE in 2018 replaced the 2016 version, and it did so with quite some effect.

[1] The interconnectedness of various information systems enables cyber incidents to spread quickly and widely. Some recent incidents have demonstrated actors' ability to penetrate the networks of large organisations and incapacitate them quickly. Cyber incidents can also spread widely across sectors and beyond geographical borders, including to entities which are not the primary target or source of disruption. Malicious cyber incidents are becoming more persistent and prevalent, illustrating the high level of sophistication and coordination that threat actors are able to achieve.
[2] For more information see details here.
[3] Available here

It sets (even if framed as non-binding guidance[4]) very comprehensive and prescriptive expectations for financial services firms – specifically also with regards to on-going risk assessments along with more detailed compliance and governance processes than perhaps may have been commonplace as well as putting cyber-resilience at the heart of various operations including when recruiting staff. The CROE also sets out what the ECB looks for in the job role and performance of a Senior Executive or the Chief Information Security Officer (**CISO**)—which may be of wider-reaching interest. CROE should be read in conjunction with rules and supervisory guidance set by other international standard setters but also by national competent authorities in the EU.

In February 2020, the ECB was awarded the Central Banking Award 2020 for payments and Market Infrastructure Development for its work on CORE. Specifically, the CROE's multi-tiered design aims to help FMIs of all sizes with strengthening their cyber-resilience as well as overseers' own capabilities and collaboration with FMIs. Moreover, the World Bank's adoption of CROE[5] and partnership with the ECB to aid global harmonisation and strengthening of the global financial system. Unfortunately, the CROE as adopted by the ECB and by the World Bank fails to define the precise threat landscape and range of bad actors that will direct cyberattacks to regulated financial services firms. In response various government policymakers have led multi-jurisdictional simulations on the impact of a major cyberattack on the global financial system[6]. The European Systemic Risk Board (**ESRB**) also published its inaugural report in February 2020 on systemic cyberattacks[7]. The ESRB's Report – in Section 2.4 (and Annex 1) specifically highlighted the common individual vulnerabilities amongst ESRB member institutions – which of course is worrying for national competent authorities inasmuch as FMIs that they are supposed to oversee[8]. With new actors (including state sponsored) using cyberattacks, a number of firms may want to revisit how they are meeting CROE and cyber-resilience more generally.

Finance is changing and cyber-security is now ever more important than ever. So too are the changes in risk management in light of the increasing shift by financial services firms to meet customers' demands for digitisation, online services, mobile applications as well as the sustained move amongst firms but their counterparts and clients towards remote and location-independent working. With rapidly evolving threat actors that are constantly adapting their tactics, techniques and procedures (**TTP**s) to remain ahead of financial services firms' defences this Client Alert assesses CROE against the backdrop of events in 2021. In addition, it is assessed in light of changes to CROE due to the EU's proposal for a new regulation for a

---

[4] It is important to note that whilst CROE's drafting is framed as non-binding – as with other similar non-binding guidance published by the ECB, CROE forms part of supervisory expectations and thus the on-going supervisory dialogue of the ECB-SSM. Equally, the CROE sets definitive expectations that relevant persons must either "meet or explain". The use of "should" in CROE, implies a "must" or "are expected to" as opposed to granting a degree of optionality – unless that divergence from the expectation can be justified.

[5] See details here

[6] Most recently on 9 December 2021 – further details available here.

[7] Available here.

[8] In 2018, the ESCG surveyed ESRB member institutions to gather information on common individual vulnerabilities (CIVs) relevant for cyber risk. Collected findings came from cybersecurity assessments undertaken by 14 ESRB members across supervised/overseen entities (including banks, FMIs and insurers). This led to the identification of the set of CIVs listed in Table 3 of the ESRB Report. The ESRB grouped these vulnerabilities into different categories according to their nature: a gap (target quality not present), a weakness (inadequate quality), a susceptibility (can be affected by something else), and a flaw (defect or imperfection). These vulnerabilities can either arise in a process or be part of a control measure. Annex 1 provides a more detailed description of each of these vulnerabilities. These include

1. Insufficient industry oversight of third-party suppliers and the supply chain – thus a weakness in process
2. Inadequate cyber hygiene – thus a weakness in process
3. Ineffective testing of people, processes and technology – a flaw in process
4. Insufficient cyber strategic planning and board level influence on cyber resilience – thus a weakness in process
5. Lack of investment in cyber threat intelligence – thus a gap in process
6. Presence of end-of-life systems – thus a susceptibility/flaw in asset
7. Technology centric focus underestimating responsibility of people and processes – thus a weakness in process
8. Organisational culture change needed for secure cybersecurity behaviours – thus a gap in process
9. Cyber undermines existing operational resilience arrangements – thus a weakness in control measures
10. High risk internet use requires better controls – thus a weakness in control measures
11. Firm scale and resource impact effective cyber-risk management – thus a susceptibility in process
12. Insufficient credible third line of defence challenge in firms – thus a weakness in process
13. Cyber maturity targets not defined – thus a gap in process

digital operational resilience act (**DORA**) which is expected to take operational effect from 2024[9]. This Client Alert should be read in conjunction with our coverage on the ECB's framework for Threat Intelligence-based Ethical Red Teaming (**TIBER EU**)[10] on 2 May 2018.

CROE's compliance objectives

The CROE was designed for use by the Eurosystem (i.e., Eurozone central banks) as part of the oversight of all payment systems. These are designated in turn as:

a) Systemically important payment systems (**SIPS**)

b) Prominently important retail payment systems (**PIRPS**)

c) Other retail payment systems (**ORPS**) and

d) The TARGET2-Securities system (**T2S**).

CROE permits national central banks, operating under national law competencies, often in conjunction with other national competent authorities to opt-in to use the CROE for any "other" FMIs—primarily this is aimed at clearing and settlement systems (including central securities depositors (**CSDs**) and central counterparties (**CCPs**).

CROE's core concepts build upon those established by the Committee on Payments and Market Infrastructures (**CPMI**) or the International Organization of Securities Commissions (**IOSCO**) and in particular their joint 2016 published "Guidance on cyber-resilience for financial market infrastructures" (the **Guidance**). CROE, however, goes beyond those principles while at the same time setting concrete steps on how to operationalise the Guidance. The 2018 version of CROE however, like its predecessor, aims to provide:

1. In-scope FMIs with detailed steps on how to embed the Guidance and improve sustained cyber-resilience over a period of time

2. Overseers with clear expectations on how to assess and monitor FMI's compliance with the Guidelines

3. The basis for common understanding and discussion amongst in-scope FMIs and relevant overseer

CROE also seeks to incorporate and hold relevant persons to comply with other standards the ECB considers best practice. Relevant firms are required to meet their "**capabilities**" i.e., the "people, processes and technologies the FMI uses to identify, mitigate and manage its cyber risks and to support its objectives."

CROE's Annex sets out a welcomingly practical and detailed Glossary of Terms. These may be useful for FMIs but also other market participants wanting to tackle cyber-resilience. This is the case even if this ECB Glossary does expand existing defined terms or even when and where it diverges from terms agreed at the international level such as by the Basel Committee on Banking Supervision (**BCBS**) or Financial Stability Board. As an example, CROE widens existing EU legal definitions and recast "Cyber incident" as:

[9] DORA incorporates the lessons that have been learned from the Eurosystem's cyber-resilience strategy for financial market infrastructures. It covers – implicitly or explicitly – the Eurosystem's cyber resilience oversight expectations, the European programme to test and improve the resilience of the financial sector against sophisticated cyberattacks (TIBER-EU), and the Cyber Information and Intelligence Sharing Initiative created by the ECRB (CIISI-EU).

[10] Available here

"A cyber event that:

1. jeopardizes the cybersecurity of an information system or the information the system processes, stores or transmits; or

2. violates the security polices, security procedures or acceptable use policies, whether resulting from malicious activity or not."

A "cyber event" is defined in CROE and very much building on EU definitions as: "Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring."

The BCBS report, unlike CROE introduced a taxonomy of cyber risk controls as part of its Annex A. These set a control objective, a control description, example control and practices and example testing approaches in relation to a number of areas. Annex B of the BCBS report set out board IT metrics which are applicable to cyber-resilience and which set out what forward-looking indicators and metrics might be useful as items to present to the Board (or equivalent governance function) of a firm. BCBS Annex C introduced concepts for a cyber-resilience metrics in terms of events and practices before a compromising event – i.e., a cyber-incident, at the point of compromise and after compromise. Many firms have borrowed from BCBS Annexes A, B and C when designing compliance monitoring frameworks to meet CROE's expectations.

CROE also communicated details on what is expected to be included in the role of a "Senior Executive" tasked with the responsibility of "owning" cyber-resilience as well as the role of a CISO (the two roles may be combined – at least from the ECB's position although other regulatory authorities may disagree). Such officers, assisted by relevant policies and procedures, are expected to foster a cyber-risk awareness culture within a relevant firm.

CROE's meet or explain approach

CROE established three levels of expectation (also referred to as "maturity levels") of how to comply with CROE's criteria or explain why they do not meet the criteria. Firms are expected and T2S as well as SIPS are required to meet and maintain at least "Advancing" maturity prior to migrating to "Innovating". While a report on CROE compliance remains non-existent, having an understanding of the maturity levels is quite important:

- **Evolving**: Essential capabilities are established, evolve and are sustained across the FMI to identify, mitigate and manage cyber-risks in alignment with the cyber-resilience strategy and framework approved by the Board. Performance of practice and capabilities are monitored and managed.
- **Advancing**: In addition to meeting the "evolving" level's requirements, practices at this level involve implementing "more advanced tools" (e.g. advanced technology and risk management tools) that are integrated across the FMI's business lines and have been improved over time to manage cyber risks posed to the FMI proactively. There is no qualitative standard in the CROE as to what constitute an "advanced" tool.
- **Innovating**: In addition to meeting the "evolving" and "advancing" levels, FMIs' capabilities across the business are identified as "…enhanced as needed in order to strengthen cyber-resilience."

In the absence of some qualitative examples as to what meets which maturity level, this left much to interpretation as well as risks of divergence approaching the meet and explain requirements quite seriously and those that merely window-dress. That in turn may mean that those embedded more fully will want to ensure they have material readily available to show to the oversight functions how they are meeting various (vaguely drafted) expectations in a concrete manner. As an example, in order to meet the innovating level, relevant in-scope FMIs are expected to demonstrate that they are "…driving innovation in people, processes and technology for the FMI and the wider ecosystem to manage cyber risk and enhance cyber-resilience." This may call for new controls and tools to be developed or new information-sharing groups to be created.

CROE adopts the approach that all relevant persons are different and thus that the means of how their capabilities meet the relevant levels will differ, the CROE is drafted in a technological, operational and jurisdictional agnostic manner. CROE is also built around the following risk management pillars as a component of an overall cyber-resilience framework that firms will need to meet or explain why they do not/cannot meet the relevant criteria:

1. Governance
2. Identification
3. Protection
4. Detection
5. Response and recovery

CROE's individual "sections"

The As a general observation, while some of what is in CROE may be familiar to a number of financial services firms, especially larger FMIs, the depth of what is documented and how may be different as the ECB's expectations may be more prescriptive. Such differences extend equally to policies and procedures but also how decisions to act or refrain from acting in a particular context are justified along with issues on data integrity.

Governance

Section 2.1 of CROE requires that firms establish a cyber-resilience strategy and framework. Conceptually some of this follows a similar approach to how the ECB-SSM communicated its supervisory expectations in transforming governance and culture in relation to non-performing loans and exposures. Firms should consider the set-up of a cross-disciplinary steering committee of senior management and appropriate staff—including (external) contractors—from multiple business units to develop a holistic framework based on threats to the firm as well as its risk tolerance for individual as well as enterprise-wide impacts is at the heart of that process and the core of building a framework. Stemming from the risk self-assessment exercise, CROE expects that organizations develop and then set their cyber-resilience strategy. This should also be aligned to its corporate strategy and its "threat landscape".

CROE also sets expectations on the involvement of the FMI's "Board" (and one presumes this extends to other forums exercising similar governance and strategic steering functions), their skills and accountability of senior management and ultimately the wider risk culture of the FMI. The Board is expected to take an active role in approving the cyber-resilience strategy and framework, setting the FMI's risk tolerance and implementation of the framework in terms of policies, procedures and controls that support the framework. As with other EU but more recently ECB-SSM rules and/or supervisory expectations (many of which read like rules) that relate to the Board and senior management, there is a need to demonstrate both individual and collective responsibility and ability. While there is an appreciation that a "senior executive" e.g., the CISO may have primary responsibility and accountability, demonstrating compliance with this supervisory outcome means having collective capabilities and taking of ownership.

In terms of compliance culture, the supervisory expectation and outcome is that relevant FMIs apply and embed a top-down as well as bottom-up approach. Again, as with the documentation aspects in Section 2.1, the distinguishing features between each of the levels are largely the deepening degree of granularity that would be expected in both the analysis of what effects a firm and the capabilities in place to maintain cyber-resilience. For FMIs that are "innovating," appointing a "cyber-expert" to the Board is one of the qualitative features. Other qualitative measures include introducing cyber-resilience and risk threat updates as a standing Board meeting agenda. In order to meet the "innovating" level, senior management is expected to cooperate proactively with other stakeholders across the ecosystem to promote a cyber-resilience culture more generally.

Identification

Section 2.2 of CROE addresses the supervisory outcomes as they relate to "identification". Specifically, FMIs are expected to identify and classify business processes and information assets that should be protected against compromise and the external dependencies. FMIs are expected to identify and document all of its critical operations and functions, key roles, processes and information assets that support those functions as well as third-party dependencies and interconnections and update that information

periodically[11]. This means having in place not only measures which aim to prevent intrusions from third-party connections and the ability to block those but also the validation of the FMI's third-party relationship management and outsourcing arrangements by an independent audit function.

This risk inventory and risk assessment should be supported by a network map showing network resources with associated IPs that locate routing and security devices as well as servers supporting critical functions as well as external linkages. Further, FMIs are expected to conduct risk assessments before deploying new and/or updated technologies, products, services and connections to identify potential threats and vulnerabilities.

CROE follows the general supervisory trend amongst international peers that relevant organizations, including senior management and their Board (i.e., taking ownership and accountability beyond the IT-staff), understand, map and manage their exposure to cyber-risk. This applies regardless of whether the connection and/or potential to exposure is connected to financial and non-financial entities. CROE also expects that external map to be reflected in understanding risks that are generated in the internal functions and thus different business units and jurisdictions and measuring both qualitative and quantitative impacts and mitigants to control risk generators and exposure threats.

Getting from "evolving" to "innovating", according to CROE, will rest on automating information feeds and data management so as to strengthen a holistic enterprise-wide risk management. The CROE however is silent on what FMIs will need to do to test the resilience and accuracy of those very data feeds and does not address the concerns of many respondents during the consultation phase that automation may actually embed and hardwire risks from programming or other shortcomings.

Protection

Section 2.3 of the CROE deals with the effective security controls, systems and processes that protect the confidentiality, integrity and availability of the FMI's assets. The measures to be implemented may be applied in a proportionate manner and should be reflective of the risk and threat landscape in which the FMIs operate. FMIs are expected to "apply a defence in-depth strategy in line with a risk-based approach." This is then clarified as meaning an FMI should implement multiple independent security controls so that if one control fails or a vulnerability is exploited, alternative controls will be able to protect the assets and/or processes that are protected and/or targeted.

In order to meet the "advancing" level criteria, the FMI is expected to develop and implement a bespoke information management system, which it states "…could be based on a combination of well-recognized international standards (e.g., ISO 270001, ISO 20000-1 and ISO 27103 etc.)". Moreover, FMIs are expected to include cyber-resilience at the outset of system design, development and acquisition process lifecycle and thus embed "resilience by design".

CROE also goes on to set out its expectations on network and infrastructure management. As a key principle, FMIs are expected to establish secure boundaries that protect network infrastructure. This includes using a router, firewall, intrusion prevention system or intrusion detection systems, virtual private networks and appropriate use of proxies as well as device connectivity. The boundaries should be split between trusted and untrusted zones, and the relevant risk profiles and criticality of information assets contained in each zone. Change and patch management processes are expected to be included in detailed policies and procedures as well as active involvement of the cyber-security team.

Logical and physical access are also addressed in this Section including in role-based access controls that allocates system access rights and privileges to specific roles. FMIs are required to review such rights periodically and take appropriate action. Interactions with suppliers and third-party security management is also touched upon in CROE. This includes due diligence on the relevant party's own systems and controls, and FMIs will need to factor that into the relevant onboarding process and risk review.

Embedding cyber-resilience into the employment recruitment and employee on-boarding process is also highlighted in the CROE as a priority area. Specifically this Section calls for screening for cyber-related incidents of prospective applicants or contractors along with regular cyber-risk and resilience training. Moving to "innovating" in the criteria set out in this Section calls for greater use of automated solutions in

[11] The CROE definition of "critical operations" builds upon that in the BCBS' Guidance and means "Any activity, function, process or service, the loss of which, for even a short period of time, would materially affect the continued operation of an FMI, its participants, the market it serves, and/or the broader financial system."

terms of processes in various lifecycle steps as well as individual steps and programs communicating with one another. CROE is equally silent here in terms

Detection

Section 2.4 discusses the expectations that FMIs will need to meet to show they have early detection capabilities to detect a potential or actual breach having taken place. Much of this Section echoes and builds upon what is set out in Section 2.1 – Identification. FMIs should have detailed incident response processes in place. Those FMIs that are "advancing" will have developed and implemented a security, information and event management system, which correlates all the network and system alerts and other unusual activity in order to detect multi-faceted attacks. This Section also sets out that FMIs should, even at "evolving" stage, establish procedures for collecting digital evidence in a "forensically acceptable manner" and maintain a "forensic readiness policy" to support forensic investigations. This may require some very technical drafting to meet both regulatory and IT-specifications.

Response and recovery

Section 2.5 deals with how FMIs should set their Recovery Point Objectives (**RPOs**) and Recovery Time Objectives (RTOs). Both of these are key in setting what point should systems be restored to in order to recommence business following a cyber-incident/attack and how quickly one can recover to that point in time. Much of what is in this Section also echoes and reiterates what is set out in the TIBER-EU Framework in terms of having computer security incident response teams. As iterated in our coverage on TIBER-EU, FMIs will have an interest in having a detailed Cyber-Response and Recovery Plan as well as escalation lists on file and in the field with the relevant colleagues.
Testing

The trend of building on the TIBER-EU Framework continues in Section 2.6 – Testing. This Section expects FMIs to have detailed and periodic vulnerability and penetration testing including using communicated scenario-based testing and a covert "red teaming" test. Moreover, FMIs are expected to develop, monitor and analyse detailed metrics of testing efficacy and regularly conduct tests in collaboration with its peers, participants and third parties in addition to industry-wide exercises to test cooperation and coordination along with communication plans.

Situational awareness and learning and evolving sections

Finally, CROE sets out what FMIs can do to monitor cyber threats both in terms of intelligence i.e., understanding the tactics, techniques and procedures of attacks along with targets as well as going a step further than the TIBER-EU Framework for those FMIs that would like to migrate to "advancing" in maintaining a cyber-risk threat dashboard. The dashboard aims to capture all threats as well as those that could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred previously.

Situational awareness also requires information sharing, and CROE considers good compliance amongst FMIs when they establish trusted and safe channels of communication with direct stakeholders for exchanging information. CROE's Learning and Evolving Section ties everything together in that FMIs are expected to place emphasis on cyber-resilience awareness to deliver on the policies an FMI has in place, as well as the CROE expectations along with how to spot and report suspicious activity.

Outlook and next steps

CROE formed a core part of the ECB, in its central banking and financial stability role, setting clear cyber-resilience expectations of FMIs but also those firms engaging with FMIs. The latter may also have additional Banking Union supervisory requirements. CROE's focus meant that FMIs and firm needed to revisit and/or expand on details in documented policies and procedures as well as how they evidence that cyber-resilience is embedded in a firm's culture as well as people and processes.

Complying with CROE also meant that a number of firms that are caught may need to ensure that they have a clear and traceable trail of justifications (including a certain degree of independent documented challenge is desirable) as to why certain arrangements have been implemented to meet CROE's expectations or why they are proportionate. Some firms may find that notably in terms of compliance

monitoring much of what CROE sets in expectations could be complemented nicely by measures set out in the BCBS Annexes to help achieve the meet or explain standard.

DORA together with TIBER-EU and CROE provides a unique opportunity to address the current fragmentation in financial legislation and supervisory approaches in the field of digital operational resilience, including cyber resilience. Firms, in particular Banking Union supervised institutions should consider performing a gap analysis between their current and future documented and operational arrangements along with what this might mean in migration plans according to the relevant maturity level along with creating linkages with other market participants.

About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from these proposals.

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via de_regcore@pwc.com or our website.

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas@pwc.com

www.pwclegal.de