The regulatory outlook for European banks in 2021 and beyond

Beyond the immediate concerns of the pandemic's impact on banks' asset quality, earnings and capital positions, supervisory authorities are focused on broader issues affecting the longer-term viability of the sector.

Banks will need to navigate an uncertain and challenging operating environment at the same time as continuing the build-up of MREL resources; further developing financial crime capabilities; strengthening and ensuring digital operational resilience; and developing a risk-based approach to climate change and environmental risks.

Minimum Requirement for own funds and Eligible Liabilities

When it comes to MREL requirements, investors have been reliant on varying public disclosures from banks, as it can be difficult to arrive at the requirements based on published policies. This stems in part from the EU's approach of assigning MREL to banks beyond those considered systemically important, as well as differences between MREL and global standards for Total Loss-Absorbing Capacity (TLAC).

The Single Resolution Board (SRB) updated its MREL policy in May 2020 to be aligned with the Bank Recovery and Resolution Directive (BRRD 2) and the Single Resolution Mechanism Regulation (SRMR 2)1. This brings about closer harmonisation of MREL and TLAC standards, especially for Global Systemically Important Institutions (G-SIIs); a new MREL based on the leverage ratio; and clarity on the level of required subordination.

In early 2021, the SRB intends to communicate MREL decisions to banks, replacing those issued previously. Each decision will comprise two binding MREL targets, including requirements for subordination: an intermediate target to be met by 1 January 2022 and a final target to be met by 1 January 2024.

As the European Union recently acknowledged in its announcement to move forward with a common backstop to the Single Resolution Fund by the beginning of 2022, the build-up of MREL buffers will be a key pillar supporting a reduction in the risk profile of the banking sector.

Financial crime

One of the more challenging aspects of bank credit analysis is assessing conduct in the area of financial crime i.e. anti-money laundering and terrorist financing. Market participants invariably only learn about incidents after the fact. We do not see this risk disappearing. As standards become more rigorous, criminals more creative, and regulators improve supervision in this area, banks will need to continue developing their financial crime capabilities.

In line with the European action plan on Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) published in May 2020[2], the European Banking Authority (EBA) is working on the infrastructure to co-ordinate and monitor AML/CFT supervision in the EU. This includes a review of the supervisory approaches used by national competent authorities and the incorporation of AML aspects into various prudential supervision guidelines.

[1] https://srb.europa.eu/sites/srbsite/files/srb_mrel_policy_2020.pdf
[2] https://ec.europa.eu/finance/docs/law/200507-anti-money-laundering-terrorism-financing-action-plan_en.pdf

Analyst

Pauline Lambert
p.lambert@scoperatings.com

Team leader

Dierk Brandenburg
d.brandenburg@scoperatings.com

Media

Keith Mullin
k.mullin@scopegroup.com

Related research

2021 Banking Outlook: first real-life stress test since post-GFC sector de-risking
December 2020

Increasing supervisory focus pushes climate risk onto bank credit agenda
October 2020

Scope Ratings GmbH

111 Buckingham Palace Road
UK-London SW1W 0SR

Headquarters

Lennéstraße 5
10785 Berlin

Phone +49 30 27891 0
Fax +49 30 27891 100

info@scoperatings.com
www.scoperatings.com

Bloomberg: RESP SCOP

In addition, qualitative and quantitative information is being gathered to build a database to foster the exchange of information between national competent authorities and support new AML colleges. This will enable the EBA to identify vulnerabilities and request national competent authorities to investigate and address them.

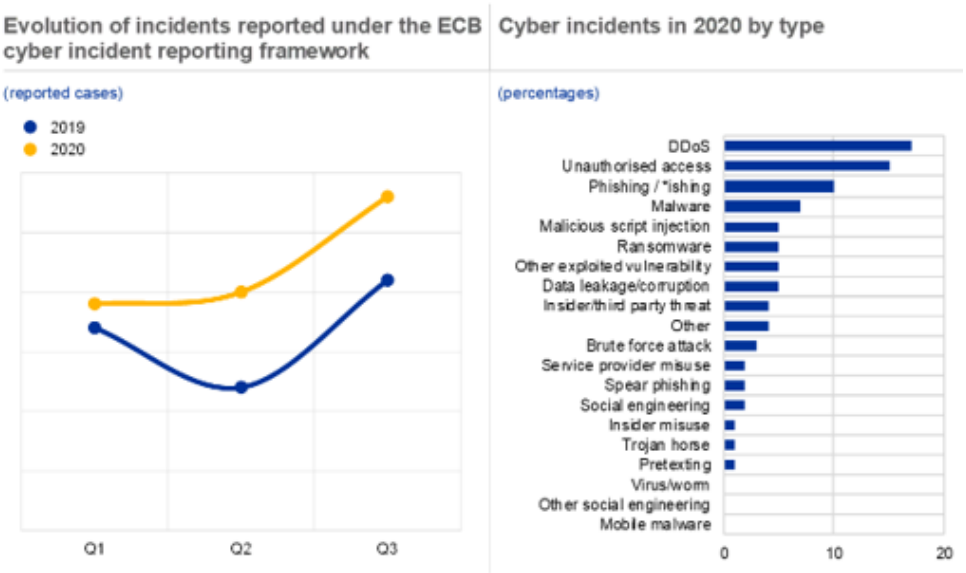
Under the fourth Anti-Money Laundering Directive, banks must apply enhanced customer due diligence for transactions involving high-risk third countries. Enhanced due-diligence measures include extra checks and monitoring to prevent, detect and disrupt suspicious transactions. The fifth Anti-Money Laundering Directive (the deadline for transposition was 10 January 2020) further clarifies the type of enhanced vigilance to be applied. As part of the action plan, the list of high-risk third countries has been expanded and will be updated more regularly.

While current EU rules on financial crime are wide-reaching, they are not consistently applied across the EU. Consequently, there is a desire to minimise divergence in several areas, including customer due-diligence requirements, internal controls, and reporting obligations. A legislative proposal from the EC to harmonise rules and establish an EU-level supervisor is expected early in 2021.

Digital operational resilience including cyber threats

The pandemic has illustrated the need for adaptable and resilient digital capabilities. Positively, banks have been to a large degree able to maintain their operations and serve clients throughout lockdowns. This does not mean, however, that banks do not need to continue investing in and developing their digital capabilities. The complexity of Information and Communication Technology (ICT) risks is increasing and the frequency of ICT-related incidents including cyber incidents is rising.

Figure 1: Frequency and type of cyber incidents



Note: Latest observation is from September 2020.
Source: ECB

Regarding cyber security specifically, European banking supervisors established a reporting system in 2017 where incidents are reported on a confidential basis and insights are shared more widely. Supervisors also encourage banks to participate in testing exercises simulating real-world attacks under the European Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU).

The EBA's guidelines on ICT and security risk management came into force on 30 June 2020[3]. The guidelines set out expectations on how financial institutions should manage internal and external ICT and security risks. These include:

(i) establishing control frameworks that clearly set out defined responsibilities,

(ii) requirements for information security to the extent that the information is held on ICT systems,

(iii) business-continuity management, including response and recovery plans, and

(iv) requirements for ICT project and change management, including the acquisition, development and maintenance of ICT systems and services.

In September 2020, the European Commission published legislative proposals on digital operational resilience as part of a broader digital finance strategy[4]. The aim is to ensure that financial firms can withstand various types of ICT-related disruptions and threats. The proposed Digital Operational Resilience Act (DORA) will for the first-time bring rules addressing ICT risk in the finance sector together into one legislative act. The proposal comprises ICT risk management, ICT-related incident reporting, digital operational resilience testing, ICT third-party risk, and information sharing.

Climate change and environmental risks

Work continues on incorporating ESG factors into the risk management of banks and supervision. In June 2021, the EBA is expected to publish a report on integrating ESG risks into the review and evaluation of financial institutions performed by competent authorities. The EBA will also prepare technical standards for Pillar 3 disclosures outlining qualitative and quantitative information on environmental, social and governance factors.

To date, governance factors remain most relevant in the credit risk assessment of financial institutions. But the importance of environmental and social factors is growing, driven by public policy, regulators, and investors. Public and investor confidence is critical for banks. Numerous ESG factors influence this perception, particularly those related to 'E' and 'S'.

These include a bank's relationships with its various stakeholders, its management of human capital (e.g. employee welfare, skill development, diversity), its impact on the environment, and its role in environmental stewardship (i.e. support for sustainable growth and investment).

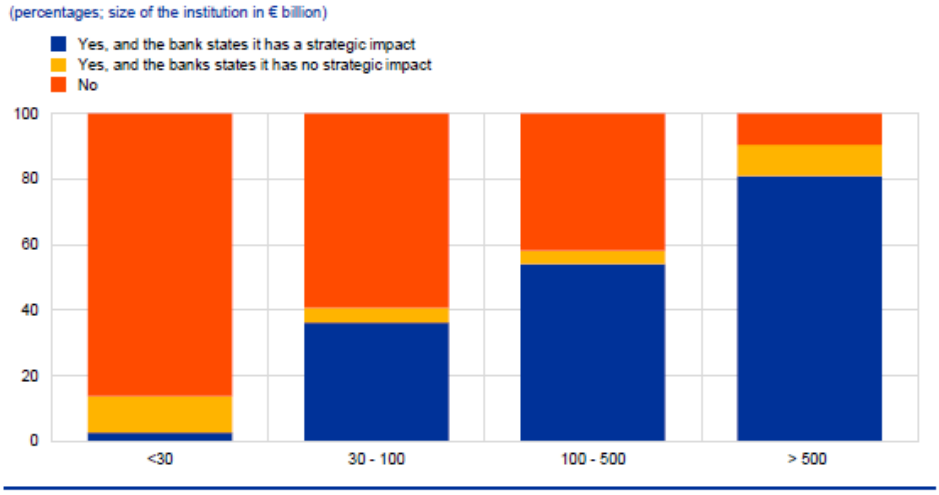
Of note, regulators are ramping up their supervision of climate-related and environmental risks. The European Central Bank's supervisory approach greatly encourages banks to assess these risks. In November 2020, the ECB issued final guidance on climate-related and environmental risks[5]. The guide details expectations for banks to consider these risks when formulating and implementing their business strategy and governance and risk management frameworks. The ECB also expects banks' disclosures to become more transparent.

[3] https://eba.europa.eu/sites/default/documents/files/documents/10180/2522896/32a28233-12f5-49c8-9bb5-f8744ccb4e92/Final%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0595
[5] https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.202011finalguideonclimate-relatedandenvironmentalrisks~58213f6564.en.pdf

The guide is not binding but serves as a basis for supervisory dialogue. In early 2021, banks will need to conduct self-assessments based on the expectations in the guide and create action plans. The ECB will benchmark these self-assessments and plans, and they will be challenged in supervisory dialogues. In 2022, the ECB will perform a full supervisory review of banks' practices, with follow-up actions to be dispensed as needed. The 2022 stress test also will cover climate-related risks.

In a separate report[6], the ECB highlighted that banks' climate-related and environmental risk disclosures were significantly lagging. In its assessment of SSM significant institutions (plus 18 less significant institutions), the ECB found that around half did not demonstrate that they had explicitly considered the potential strategic impact of climate-related risks. For those institutions that deemed the risks to be immaterial, this could not be verified based on the information disclosed. Clearly, the ECB expects banks, particularly smaller ones, to do more in this area.

Figure 2: Disclosures on climate-related risks and their materiality



Source: ECB

[6] https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.ecbreportinstitutionsclimaterelatedenvironmentalriskdisclosures202011~e8e2ad20f6.en.pdf

Scope Ratings GmbH

Headquarters Berlin
Lennéstraße 5
D-10785 Berlin

Phone +49 30 27891 0

Frankfurt am Main
Neue Mainzer Straße 66-68
D-60311 Frankfurt am Main

Phone +49 69 66 77 389 0

Paris
23 Boulevard des Capucines
F-75002 Paris

Phone +33 1 8288 5557

London
111 Buckingham Palace Road
London SW1W 0SR

Madrid
Paseo de la Castellana 95
Edificio Torre Europa
E-28046 Madrid

Phone +34 914 186 973

Milan
Regus Porta Venezia
Via Nino Bixio, 31
20129 Milano MI

Phone +39 02 30315 814

Oslo
Karenslyst allé 53
N-0279 Oslo

Phone +47 21 62 31 42

info@scoperatings.com
www.scoperatings.com