Skadden

Cybersecurity and Data Privacy Update

July 16, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

ECB Mandates Board Expertise in Addressing ICT and Security Risks

Earlier this year, a dedicated policy prepared by the European Central Bank (ECB) came into effect requiring bank management bodies to broaden their collective understanding of and proficiency in identifying and dealing with information and communication technology (ICT) and security risks.

This policy, which came into effect in March 2024, has its roots in the Single Supervisory Mechanism (SSM) goals for 2024–2026 and embodies the ECB's commitment to overseeing the implementation of robust operational resilience frameworks within financial institutions. The policy emphasizes the need for banks to actively manage risks related to the increased digitalisation of the banking sector while also embracing technological innovation.

The regulatory trend in Europe — illustrated in the new Network and Information Security (NIS2) and the Digital Operational Resilience Act (DORA) regimes for increased cybersecurity — is that management bodies and boards need to be engaged with ICT risk and risk management and cannot delegate this to chief information security officers or other functions. They must have robust incident response plans and have comprehensive and regular training on implementing these plans. Significant ICT incidents, whether caused by a cyber attack, technology failure or an internal mistake, are a board issue, and boards must be ready and proactive in dealing with them.

See our 2 November 2023 client alert "DORA – Key Considerations for Alternative Investment Funds."

Key Points

In order to determine how prepared bank management bodies are to recognize and address ICT and security risks, the policy states that, as part of "fit and proper assessments" the ECB conducts, it expects that:

- **Management bodies must have sufficient understanding of ICT and security risks:** Members of a bank's management body and internal control functions, such as risk management, compliance and audit, must be sufficiently knowledgeable about ICT and security risks alongside data and reporting requirements.
- **There should be a board member with practical cyber experience:** Banks should have at least one non-executive board member possessing recent practical expertise in ICT and security risks. The ECB suggests that five years of practical experience is an adequate threshold.
- **Regular training of management body members is expected:** Management body members should undertake regular training (at least annually) to maintain up-to-date knowledge and skills regarding ICT and security risks. In light of the incoming Digital Operational Resilience Act (DORA), which is discussed further below, the ECB encourages banks to start this annual training in 2024.

© Skadden, Arps, Slate, Meagher & Flom LLP. All rights reserved.

Failure to demonstrate that a management body member is, or remains, fit and proper may result in the ECB rejecting their appointment (or reappointment) to a bank's management body, or imposing conditions on their appointment, though the exact procedure differs between EU member states.

While the ECB's policy does not create new obligations, it clarifies the ECB's interpretation of existing obligations in relation to fit and proper assessments, and reiterates the ECB's focus on cyber risks. In addition, although the ECB only regulates certain key banks under the Single Supervisory Mechanism, the policy will inform the approach of national banks and other EU financial regulators undertaking similar assessments under their respective regulatory frameworks.

The expectations outlined in the ECB's policy will be applied by the ECB with the principle of proportionality in mind. This means that, when applying the "fit and proper assessment", the ECB will take into account factors such as the size of the bank, its exposure to ICT and security risks, and the specific management position being evaluated. Additionally, although the ECB sets out some benchmarks (such as yearly training and five years of cyber experience), the policy will be applied on a case-by-case basis, allowing for flexibility and adaptability to different banking environments and scenarios, in line with the principle of supervisory judgement.

Overlap With DORA

The ECB has stressed that, whilst its policy sets expectations for banks regarding ICT and security risks, it is not designed to supersede or conflict with any legal requirements at the national or European level, such as DORA, which will apply from 17 January 2025.

DORA similarly requires actions related to digital operational resilience, including mandating the allocation of a budget for ICT security awareness programs and training and regular refreshes of ICT risk knowledge. DORA also requires staff training tailored to roles extending to senior management, and the integration of operational conclusions into risk assessments following cyber incidents, with tailored training development as necessary. Moreover, DORA extends training requirements to a company's third-party ICT service providers.

Together the ECB's policy and DORA aim to strengthen the resilience of financial entities against cyber threats. However, whilst the ECB's policy particularly focuses on the knowledge and expertise of internal stakeholders, DORA mandates specific actions, budget allocations and training requirements to ensure comprehensive readiness and resilience at a broader scale. The ECB's policy is therefore a tool which banks can and should use to demonstrate their capabilities in responding to dynamic ICT and security risks and should be implemented alongside any other legal requirements banks may be subject to, including DORA.

What To Do Now

In order to comply with the new ECB policy, and in preparation for DORA, which will come into effect in January 2025, banks within the EU should:

- Consider what would constitute the management body or board for the purposes of the ECB policy and DORA.
- Establish board oversight of ICT risks by ensuring regular briefings.
- Ensure incident response plans and playbooks are comprehensive and in line with regulatory requirements, recognizing and planning for the role of boards in incidents.
- Implement a comprehensive training programme for boards on ICT risks and run a variety of tabletop exercises practicing board oversight and considering different risks and their impact on the business.

The EU's Digital Operational Resilience Act (DORA) – 2024 Update

Contacts

Nicola Kerr-Shaw
Counsel / London
44.20.7519.7101
nicola.kerr-shaw@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Imad Mohammed Nazar
Trainee Solicitor / London
44.20.7519.7649
imad.nazar@skadden.com

William E. Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Susanne Werry
Counsel / Frankfurt
49.69.74220.133
susanne.werry@skadden.com