COENOBIUM ADVISORS

Governance and Bank Technology Risk in a Dynamic Global Environment

Claes Norgren | Juan Perez Calot | Tom Loughlin | Damian Robinson

I. Introduction

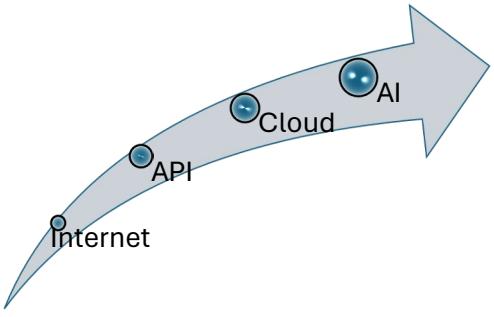
The supervisory boards and management bodies of banks and other financial institutions today are at the crossroads of *technological change* and transformation, intensified *regulatory requirements* for operational and technology risk, and a dynamic, technology-driven *risk landscape*. Boards managing these challenges need to define a comprehensive long-term strategy and implement solutions that involve not only investments in technology itself, but increasingly in specialized risk management capabilities, in governance frameworks, in staff competencies, and more specifically in establishing a fit-for-purpose risk culture.

II. Technology developments, new banking services, opportunities and risks

Recently, the European Union decided upon the first artificial intelligence legislation, setting out a risk-based approach for the development and use of AI.[1] This is a clear example of how technology impacts regulations and the business environment, and nowhere is this relationship more evident than in the banking and financial services industries.

The impact of technology on banking has been high on the regulatory and management agenda for many years, and this trend will likely accelerate. Technology has changed the costs of production and distribution of services, has enabled the development of new services and new markets, and has allowed the customer experience to be improved dramatically. Consider when the last time was that you had to stand in a long queue at your local bank branch to execute a simple cash or payments transaction.

Certain technological advances in recent decades have been particularly important for the banking and financial sectors. These include the proliferation of internet banking, the deployment of remote and web-based application programming interfaces (APIs), the advent of cloud computing, and most recently the emergence of machine learning and artificial intelligence (ML/AI) applications. Among other things, these developments have transformed banking and have enabled:



- ✓ Operational transformation, new business models, and the widespread application of outsourcing arrangements, providing new possibilities for improved business scalability;
- ✓ New product types (including more complex transactional capabilities) and delivery channels—e.g., digitalization, faster payments, and Open Banking;
- ✓ Improved security practices in relation to authentication, identity management, and operational resilience; and
- ✓ New tools and capabilities for compliance, risk management, and internal audit.

At the same time, the effects of technological developments on the risks faced by banks and other financial entities have been profound. Previously understood risks have changed qualitatively and new risks related to the use of technology continue to emerge. For example, while technologies designed to help optimize the

[1] "Shaping Europe's digital future," European Commission, March 6, 2024. URL: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

efficiency and effectiveness of risk and compliance functions—from advanced AML screening and investigation tools to robust cybersecurity measures to help mitigate against fraud and protect customers' transactions—have largely made a positive contribution to the safety and security of financial institutions, some of the very same technologies have also created new challenges. Fraudsters and other criminals with access to new products can use these technology-based tools and methodologies to more easily obscure their identities and exploit vulnerabilities in the financial system.

Likewise, digitalization—with its new transaction patterns, infrastructure requirements, and higher security standards (e.g., the implementation of eIDAS 2.0 in the EU)—has led to increased operational efficiency in the form of higher levels of process automation, cloud-based web services, and opportunities to use digital identities for remote customer onboarding. It has also been one of the drivers of the near-universal trend towards the increased movement of data and processing activity beyond the confines of financial institutions' own data centers and into the hands of a variety of third-party providers. These include cloud service providers, software-as-a-service providers, traditional bank servicers (many of which are themselves moving to cloud infrastructure, compounding third-party risk even further), as well as fintech, payments-as-a-service, and banking-as-a-service partnerships in the context of Open Banking.

The extended perimeter and growing ecosystem of third-party processing and service relationships can entail heightened downside risks, as well. Under conditions of financial stress, for example, a bank's outsourcing arrangements can impact operational and/or liquidity risk and can lead to concerns about financial stability. Meanwhile, new threats are on the rise from cyber attacks through banks' and their partners' communication networks and transactions with clients. These phenomena have resulted in the need for more sophisticated business continuity and recovery plans and for improved cyber risk management frameworks. Even banks that maintain largescale on-premises IT infrastructures are finding that more and more of their technology risk management efforts are becoming intertwined with third-party risk management issues.

New risk management tools and metrics have thus become necessary in order to identify, assess, and mitigate more complex and emerging threats, as well as generally to better handle technology-related and third-party risks. Banks that learn to measure the impact of technology operations on risk exposures more effectively, and which expand their portfolio of risk-mitigation techniques and proactively manage their risk appetite stance in new and often unfamiliar areas, are better positioned both to take advantage of, and to protect themselves against the risks of, new and emerging technologies and the business trends they engender. These developments are increasingly being incorporated into banks' enterprise risk management frameworks as best practices.

III. Evolving regulatory requirements

The dynamic risk landscape described above has prompted regulators around the world to respond by developing a variety of burgeoning regulatory frameworks aimed not only at promoting financial stability, while at the same time allowing banks to exploit new technology applications in ways that are considered safe for the financial system, but also at addressing the intersection of the financial industry with Information Communication Technology (ICT) infrastructure. For example, the Basel Committee on Banking Supervision (BCBS) has been at the forefront of the development of a capital regulatory framework and other standards that emphasize the governance of technology related risks, while at the European Union level, a new regulatory landscape has emerged in the form of directives and regulations aimed at addressing specific risk areas. In other regions, such as the Middle East, developments are in motion that will allow regulators to evaluate and leverage what has worked well in other parts of the globe.

In keeping with the pace of technological change, this process has accelerated in recent years to cover a number of critical areas with important new regulatory initiatives, such as:

- *Data privacy,* protecting both individuals and companies*;*
- *Prudential risk,* enhancing financial stability through requirements related to operational risk;
- *Technology-specific regulations,* focusing not only on risks to the financial sector and new threats related to cyber and information security, but also addressing social objectives.

Compliance with these regulations is often complex, particularly for financial institutions operating across borders, and this can contribute to heightened regulatory risks. In this context, national and supranational supervisors alike have begun to focus more on banks' boards of directors and on how they set the "tone from the top" and the institutional governance frameworks to promote accountability within the risk cultures of their organizations.

IV. Importance of Risk Culture and Control Environment

When implementing governance, risk, and compliance arrangements driven by the developments outlined above, it is key for institutions to do so within the context of the specifics of the organization and its people. Professionals leveraging specialized risk management tools often need to interact in new ways, and this 'people' dimension of risk governance is crucial for the long-term success of transformation efforts and their positive impact on the three lines of defense.

> ***"Institutions should develop an integrated and institution-wide risk culture, based on a full understanding and holistic view of the risks they face and how they are managed, taking into account the institution's risk appetite."***[2]

The bar set by regulators is high: Supervisors expect institutions to develop a risk culture—through policies, communication, and training—that is embedded in their activities, their strategies, and their risk profiles. For risk, compliance, and technology professionals, these new ways of working require seamless cooperation through the development of common reporting standards and the alignment of processes. That is a significant challenge in any institution, and banks need to pay close attention to a number of drivers of success, including:

1. Facilitating a seamless interaction between business units, technology, risk, and compliance, to enable the bank to effectively understand, measure, monitor, contain, and report on its risks;
2. Understanding and ascertaining appropriate ways to measure risk exposures, especially those impacted by technology- and third-party-related risks;
3. Defining and implementing proper internal controls to ensure risk exposures are maintained within established profiles and targets and that residual risks are minimized.

[2] Guidelines on internal governance under Directive GL 2021/05, *European Banking Authority.*

For many banks and financial entities, significant investment is required in order to build these competencies, to establish an appropriate risk culture, and to provide the necessary enabling tools and methodologies. Boards of directors must understand the importance of these items on the strategy and governance agendas.

Additionally, new requirements related to technology can lead to more complex interactions with various stakeholders at the operational levels of the bank. It is therefore critical from a board perspective to set the right tone at the top, to establish and enforce accountability in governance structures and processes, to promote adequate communication between the board and management bodies, to facilitate opportunities for appropriate challenge, and to implement effective incentive structures. When selecting directors, it is particularly important to nominate board members who are sufficiently technology-savvy.

V. Board practices

One of the key roles of a bank's board of directors is to participate in setting, monitoring, and constructively challenging the strategy of the institution. Boards therefore need to be in a position to continually review and update their planning and business models in light of new technologies at play, as well as changed competitive and risk landscapes. This involves assessment of how new technologies will be implemented and their impact on markets.

DORA Governance Requirements for Boards of Directors

- Oversight: Boards are required to take an active role in the governance of ICT and digital risks, including understanding and approving the financial entity's ICT risk appetite and strategy.
- ICT Risk Management Framework: Boards must ensure the implementation and maintenance of a sound, comprehensive, and well-documented ICT risk management framework.
- Testing and Reporting: Boards are responsible for ensuring the regular testing and auditing of the effectiveness of the entity's ICT risk management framework. They must also ensure that significant cyber threats and incidents are reported to the relevant external authorities.
- Training and Awareness: Boards must promote a culture of digital operational resilience. This includes ensuring that board members themselves and the relevant staff members of the organization receive regular training on ICT risks.
- Review and Approval of Policies: Boards are responsible for reviewing and approving policies related to the management of ICT, including those on digital operational resilience.
- Incident Management: Boards have a role in overseeing the response and recovery processes in the event of major ICT-related incidents, ensuring that actions are taken swiftly to mitigate any negative impacts.
- Compliance: Boards must ensure the institution's compliance with DORA's requirements, including the management of risks related to third-party ICT service providers.

Board governance also needs to embed supervision of the bank's operational activities from a holistic technology-risk perspective. This includes several specific areas, such as ensuring adequate controls over outsourcing and third-party IT strategies, information security, and data privacy practices. It also means that a high level of attention must be given to the adequacy of reporting processes, the embedding of the ICT risk framework into the overall enterprise risk framework, the robustness of business continuity plans (including testing), and increasingly the effectiveness of cybersecurity and operational resiliency capabilities.

Throughout the European Union, the new Digital Operational Resilience Act (**DORA**) regulation[3] is set to apply beginning in January 2025, affecting twenty (20) different types of financial entities.[4] Its implementation requires strong internal

[3] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022, Official Journal of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

[4] These include banks, insurance companies, and investment firms, among others.

governance arrangements, proper control frameworks, and the full commitment of boards of directors and governing bodies of affected institutions to planning and managing the implementation of the regulation's requirements. DORA establishes standards for a range of new policies, new reports, and the review of internal procedures and controls related to the financial institution and its IT providers. Boards and governing bodies will therefore need to review, analyze, challenge where appropriate, and approve a variety of matters related to risk management frameworks, outsourcing policies, and others. Similar requirements have also been introduced in other jurisdictions, such as the recent US interagency guidance on third-party relationship risk management.[5]

From a practical perspective, this translates to several questions concerning boards of directors and governing bodies of financial institutions, which are important for shareholders, supervisors, and other key stakeholders to address. Foremost among these are:

- ✓ How best to ensure the appropriate composition of the board in relation to technical competencies, and to select the right board members and effectively manage board and committee meetings?
- ✓ How can the board best design its committee structures, governance mandates, and operating procedures to deal effectively with technology issues?
- ✓ How can boards be provided with appropriate levels of support (e.g. through training, information flows, and other conditions for optimizing decision making) to achieve the right levels of ongoing competence and understanding around technology-related issues?
- ✓ And how should boards best ensure that a sufficient share of management's mind and resource allocations are aimed at the proper assessment and response to increasing third-party dependencies?

VI. Conclusions

Banks and other financial institutions have their own sets of challenges that are unique to their operating realities, risk landscapes, and business models. Each organization is at a different point on its maturity journey, but the target destinations are all similar. They each want to be in the best position to leverage new technological developments safely, efficiently, and to operate in compliance with their regulatory frameworks, for the benefit of their businesses and their customers. The measures needed to address these challenges effectively are based on leveraging international best practices and on engaging advisors that are practitioners who have met and overcome these challenges in diverse markets.

Based on our practical expertise and drawing on our trusted network of specialized technology partners, COENOBIUM ADVISORS can help financial institutions assess the risks, challenges, and gaps they face and can assist them in developing robust and efficient roadmaps to setting and achieving their technology risk governance goals.

About COENOBIUM ADVISORS

COENOBIUM ADVISORS is a team of expert Governance, Risk, and regulatory Compliance (GRC) professionals, with a core focus on the financial industry. Our advisors are seasoned practitioners with an average of 25+ years' experience working with top-tier financial institutions, consulting firms, and supervisory authorities. We partner with consulting and technology firms, providing international expertise on GRC-related engagements. For more information about us, see our website at: https://coenobiumadvisors.com.

© Coenobium Advisors, May 2024

[5] See: "Interagency Guidance on Third-Party Relationships: Risk Management," *Federal Register 88 FR 37920*, June 9, 2023. URL: https://www.federalregister.gov/d/2023-12340.