



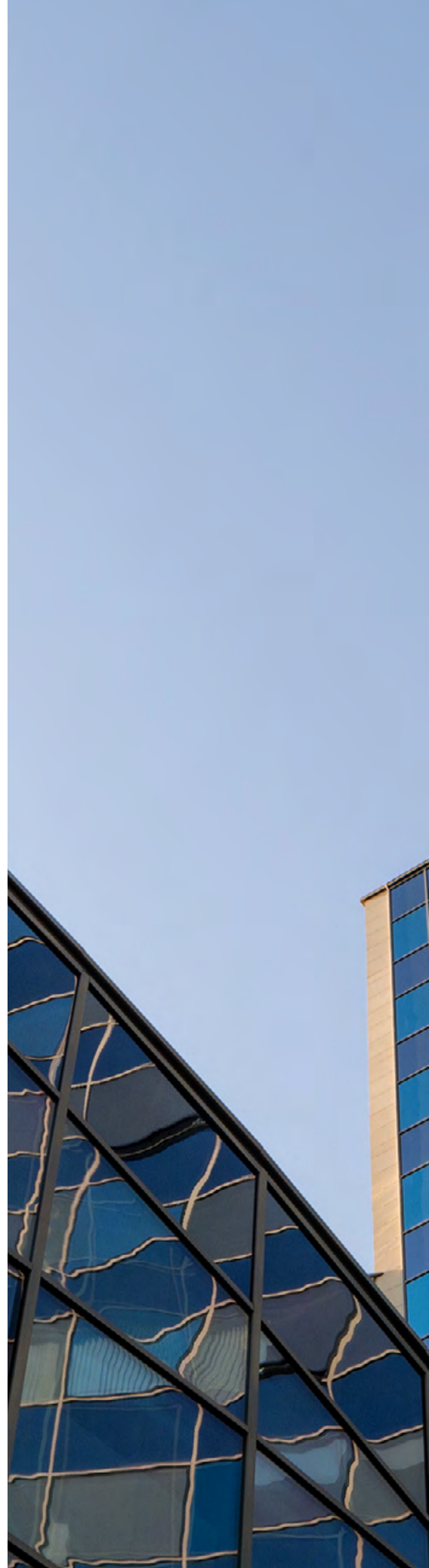
Considerations for the boardroom of credit institutions 2024



November 2024

Content

Executive summary	3
Digital Operational Resilience Act (DORA)	4
The EU's AML Package is finally here	7
ESG disclosures	13
From anti-money laundering to anti-tax crime laundering: can you manage your tax risks?	17
Digital Transformation in Banking	19
From open banking to open finance	23
Elevating CX: a strategic priority for banking in 2025	28
CRR III & CRD VI	35
Markets in crypto-assets regulation (MiCA)	40
New investment tax credit	43
Banking Data Strategies: Leveraging Data Governance, Cloud Implementation, and Data Fabric Architectures	48
Artificial intelligence governance in Banking	53
EMIR Refit	57



Executive summary

We're delighted to share our first edition of *Considerations for the boardroom of credit institutions*, a toolkit for the banking industry's hottest boardroom topics. We believe this guide will boost the quality of your boardroom discussions.

Alongside a brisk overview of the leading boardroom topics, we've also included questions to help you uncover the bank's status regarding these crucial matters.

We will regularly update this toolkit to capture the evolving regulatory agenda and our market insights.

We wish you a pleasant and insightful read.

KPMG

Digital Operational Resilience Act (DORA)

Effective since January 2023, DORA is the EU's regulatory framework for managing information and communications technology (ICT) and supplier risks. It aims to improve the financial sector's ability to withstand and recover from disruptions and threats.

A crucial component of the European Commission's digital financial package, DORA's primary objective is to ensure that financial market participants can maintain safe and reliable operations, even in the face of significant ICT disruptions.



Banks and other financial institutions have been granted a transition period until 17 January 2025 to achieve full compliance.

In Luxembourg, the Commission de Surveillance du Secteur Financier (CSSF) is actively preparing the market for DORA in several ways, including:

- **Legal developments:** Luxembourg's "DORA law", published on 1 July 2024 and effective from 17 January 2025, aligns national financial sector laws with the EU's DORA regulation, empowering national authorities with necessary supervisory and investigative powers.
- **Regulatory developments:** CSSF Circular 24/847 introduces a new ICT-related incident reporting framework to tackle the growth of ICT and security risks in a highly interconnected global financial system. It aims to gain an improved and more structured overview of the nature, frequency, significance and impact of ICT-related incidents, and its requirements partially overlap with DORA's.
- **Raising awareness:** the CSSF has already given several presentations on DORA, including to professional associations and in other market forums.

What is required?

DORA sets out a comprehensive framework for managing risks linked to the financial sector's growing digitalization and the dynamic cyber threat landscape. So, what steps must banks take to comply?



Governance and organization <ul style="list-style-type: none">• Create a comprehensive ICT risk management framework to ensure resiliency, enabling the identification, assessment, management and monitoring of ICT risks• Ensure the bank's management body is ultimately responsible for achieving digital operational resilience.	Digital operational resilience testing <ul style="list-style-type: none">• Create a risk-based digital operational resilience testing program as an integral part of the ICT risk management framework• Perform advanced testing based on threat-led penetration testing (TLPT)• Implement requirements for testers carrying out the TLPT.
ICT risk management framework <ul style="list-style-type: none">• Ensure all sources of ICT risks are identified, assessed, managed and monitored• Protect ICT systems and detect anomalous activities• Implement response and recovery plans and procedures.	Managing third-party risk <ul style="list-style-type: none">• Establish ICT third-party risk as an integral part of the ICT risk management framework• Create a strategy for ICT third-party risk• Establish a register of information• Perform pre-contracting analyses of ICT services• Promote standard contractual clauses
ICT-related incident management, classification and reporting <ul style="list-style-type: none">• Implement an incident management process and monitor ICT-related incidents• Classify ICT-related incidents and cyber threats• Report major ICT-related incidents to authorities.	Information-sharing arrangements <ul style="list-style-type: none">• Reinforce the legal grounds for information-sharing arrangements on cyber-threat data and intelligence.

Questions that may be raised

1

Have we defined a digital operational resilience (DOR) strategy that's integrated with other strategic documents, such as the IT and outsourcing strategy?

4

Do we comprehensively understand our ICT dependencies, including all ICT assets and any direct or indirect ICT third-party service providers?

2

Have we conducted a gap analysis against DORA's requirements?

5

Has a budget been allocated for DORA compliance?

3

What challenges could we face when implementing DORA's requirements, including sufficient understanding and mobilization at the group level?

6

Has a person or team been designated to follow the evolution of future regulatory technical standards (RTS), implementing technical standards (ITS) and guidelines underpinning DORA?

By

Onur Ozdemir

Partner, Tech & Cyber Risk Consulting
E: onur.ozdemir@kpmg.lu

Ashish Bedi

Director, Tech & Cyber Risk Consulting
E: ashish.bedi@kpmg.lu

The EU's AML Package is finally here

In July 2021, the European Commission presented an ambitious suite of legislative proposals to strengthen the EU's anti-money laundering (AML) and countering the financing of terrorism (CFT) rules, commonly known as "the AML Package". After more than two years of negotiations, the European Parliament adopted the AML Package on 24 April 2024.

The AML Package consists of three legislative instruments¹:

- The EU Single Rulebook REgulation (AMLR)
- The Anti-Money Laundering Authority Regulation (AMLAR)
- The sixth Anti-Money Laundering Directive (AMLD 6)

The AML Package's key developments include:

The AMLR (currently in effect and applies as of July 2027).

- This single rulebook legislation aims to harmonize approaches across EU Member States. Unlike a directive, the regulation directly applies to Member States and does not require transposition.

It enforces EU-wide rules on:

- Scope of obliged entities
- Internal policies, controls and procedures of obliged entities
- Customer due diligence
- Beneficial ownership transparency
- Reporting obligations
- Record retention
- Measures to mitigate risks deriving from anonymous instruments.

The threshold to determine beneficial ownership in corporate entities has been set at 25%. However, Member States may identify categories of higher-risk corporate entities and propose a lower threshold, which should not fall below 15%.

- **The AMLAR** (currently in effect and applies as of July 2025)

¹ The recast of the Transfer of Funds Regulation, initially part of the AML Package, was uncoupled and adopted separately in June 2023.

The AMLAR establishes an AML competent authority at the EU level known as the Anti-Money Laundering Authority (AMLA).

AMLA will be:

- Seated in Frankfurt am Main, German.
- Accountable to the European Parliament and the Council for the AMLAR's implementation.

From 2028, one of AMLA's key roles will be directly supervising at least 40 selected obliged entities and indirectly supervising non-selected obliged entities.

The AMLD 6 (currently in effect and must be transposed into Member States' legislation by 10 July 2027). The directive sets, amongst others, enhanced rules regarding beneficial ownership information and its recording in Central Registers.

While the AMLR will only apply from July 2027 and the AMLD 6 still requires transposition, financial institutions should assess the AML Package's impact on their operations and start preparing. KPMG's dedicated team of AML and CFT specialists is ready to support you in this journey.

The rising cost of financial crime compliance

A LexisNexis Risk Solutions study revealed that financial crime compliance costs increased for an overwhelming 98% of EMEA financial institutions in 2023, who collectively spend over US\$85 billion annually on these efforts².



Significant increase in technology-related costs

Technology costs regarding networks, systems and remote work have risen at 70% of organizations in EMEA and 67% in Europe. Most of these costs were for compliance and know-your-customer (KYC) software.



Emerging risk of cryptocurrencies, digital payments and artificial intelligence (AI) technologies

Twenty-nine percent of financial institutions indicated that evolving criminal threats are the most significant factor driving an increase in financial crime compliance costs. This is surpassed only by the costs related to financial crime regulations and regulatory expectations (38%), and the increased requirement for automation, data and tools (32%).



Increasing labor costs

Seventy-two percent of organizations' labor costs related to full-time employees and part-time salaries have risen over the past 12 months.

² Kangkan Halder, "[98% report rising financial crime compliance costs: survey](#)," *Delano*, 19 March 2024

Since January 2024, the CSSF's total cost of administrative sanctions was estimated at €3.2 million, of which €3 million involved a credit institution's non-compliance with AML and CTF professional obligations.

Source: CSSF

In July 2023, the US Federal Reserve imposed a US\$186 million fine on Deutsche Bank and its US affiliates for inadequately addressing AML control deficiencies, following previous regulatory concerns.

Source: Reuters

In February 2024, the US federal judge approved a plea deal by one of the world's largest cryptocurrency exchanges to pay more than US\$4.3 billion in fines and restitution, after pleading guilty to breaking AML laws and violating sanctions.

Source: CSSF

It's important to remember that in addition to direct expenditures like staffing and screening, monitoring and reporting technology, the true cost of compliance also includes potential administrative fines from regulators. As the old saying goes: if you think compliance is expensive, wait and see how much non-compliance will cost you.

Out of the CSSF's 29 administrative sanctions published in the first half of 2024, more than a third were regarding non-compliance with AML and CFT obligations. While the severity of the penalties varied from reprimands and official warnings to a €3 million fine, the banking sectors' sanctions fell at the higher end of the spectrum.

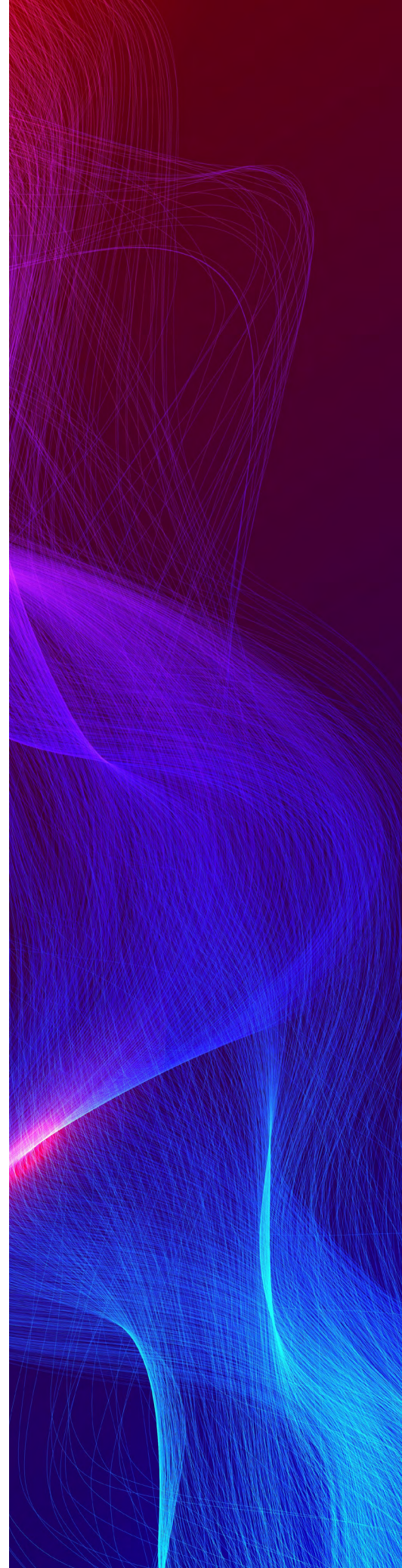
In comparison, foreign regulators' administrative sanctions, particularly those in the US, often surpass the CSSF's, with fines reaching several billion US dollars in exceptional cases.

While these figures alone are noteworthy, the costs of associated remediation programs, external monitors and supplementary inspections can often exceed the penalty itself.

Finally, there's a cost that can be harder to quantify - the one of lost opportunities. Lengthy onboarding processes and unnecessarily blocked accounts and transactions can lead to poor customer experience (CX) and missed business opportunities.

The most suitable way to control financial crime costs depends on the organization's business and operational model, existing AML/CFT framework, and risk appetite. Popular solutions include automation and technology, first-time-right strategies, lean processes, and outsourcing and co-sourcing.

Don't hesitate to reach out to KPMG to discuss your unique needs. We offer cost-effective, technology-driven solutions that shrink turnaround time, coupled with experienced resources in a wide range of financial crime matters.



Questions that may be raised

1

Have we prepared for the changes of the EU's AML Package?

4

Do we lack inhouse AML and CFT expertise or resources?

2

Are we considering a cost-effective and technology-driven solution that reduces turnaround time?

5

Are we struggling to meet our deadlines regarding initial and ongoing due diligence cycles?

3

Do we have a growing backlog of due diligence files to review?

6

Are our procedures adequate and in line with AML and CFT requirements?

By

Giovanna Giardina

Partner, Advisory - Forensic and AML

E: giovanna.giardina@kpmg.lu

Michal Pochec

Director, Advisory - Forensic and AML

E: michal.pochec@kpmg.lu

ESG disclosures

While financial institutions are well used to complying with different regulations, responsible banking's dynamic and fast-paced regulatory landscape requires multiple reporting disclosures that banks must prepare for.

To meet consumers' growing demand for transparency and accountability, banks must prioritize their environmental, social and governance (ESG) practices. Here are the main ESG and sustainability challenges that banks face, and the steps to tackle them:

Put my ESG strategy into motion

How can I define an ESG strategy and put it into practice?

Adapt my operating model to address ESG opportunities

How should I update my operating model to comply with the integrated regulatory framework and create value?

Report according to the SFDR's final RTS

How should I address the reporting requirements of the final RTS?

Required disclosures: what are they, and why are there so many?

Banks must disclose a range of information on their ESG practices, which differ based on purpose and content type.

- The **Corporate Sustainability Reporting Directive (CSRD)** complements an institution's annual financial report to promote sustainable investment and firms' accountability toward ESG practices. Banks must define their ESG goals and disclose their progress using qualitative and quantitative measures.
- The **EU Taxonomy Regulation** sets the criteria for calculating banks' green asset ratio (GAR), which **measures the proportion of their assets aligned with the EU Taxonomy**. The aim is to guide banks' investments towards green initiatives and allow investors to view their contribution to environmental objectives.
- The **Sustainable Finance Disclosure Regulation (SFDR)** sets requirements for financial market participants to disclose sustainability information. This helps **investors make informed choices based on companies' sustainability profiles** and how they manage and account for sustainability risks in their investment decision process.
- The second **Markets in Financial Instruments Directive (MiFID II)**, in particular Article 9(13) of the MiFID II Delegated Directive, ensures that distributors understand, recommend and sell financial instruments to the appropriate target market and **meet clients' expectations regarding their sustainability preferences**.



- Article 449a of the **second Capital Requirements Regulation** (CRR II) added ESG risks to the Basel framework's Pillar 3 **reporting requirements**. The aim is to promote market discipline by enhancing the transparency and disclosure of banks' ESG risk exposures and risk management practices.
- The **Partnership for Carbon Accounting Financials (PCAF) guidelines** enable the **accurate tracking and reporting** of financed emissions, **helping banks meet their sustainability goals** and improve transparency with stakeholders regarding scope 3 carbon emissions. It also supports risk management by identifying carbon-related exposures and aligning with global climate targets.
- Under **CSSF Circular 21/773**, banks must identify, measure and monitor their exposures to climate-related and environmental risks. They are required to **collect data and perform balance sheet stress exercises that take negative scenarios on climate and environmental factors into account**. While this Circular prescribes enhanced internal processes to calculate and monitor these exposures, it doesn't prescribe any additional public disclosures than those covered in this section.

Key challenges raised

The major hurdles faced by banks include:

- The **unprecedented variety and amount of new data points** that banks must collect and process on their counterparties, products, partners and providers. Over 500 data points are required to publish these disclosures, based on a sample of banks' exercises. This requires banks to analyze and implement new data collection processes, uses, storage and controls to manage this volume.
- The **sheer number of internal stakeholders impacted** by these disclosures' requirements. This includes the banks' front-office teams in charge of client relationships and the products offered; the second and third lines of defense; the top management; and departments like facilities, data office and HR.

As banks adapt to comply with these ESG considerations and disclosure requirements, they must apply good governance principles and coordinate with all relevant stakeholders to prepare for these new standards.

Questions that may be raised

1

As board members, what is our collective understanding of responsible banking and integrating ESG considerations into our day-to-day business, operations and acquisitions?

5

Are our databases and data collection processes ready to manage the increased amount of new data?

2

Have we identified our ESG ambitions? Should existing products be adapted, and are there opportunities for new products? How should we measure our ambitions?

6

Have we assessed third-party providers to supply the required data and support us in the reporting process?

3

Have we identified the disclosure information required as of January 2023? Were we able to produce all related information? Are we ready for the upcoming disclosures, or is there any difficulty foreseen in the collection and reporting process?

7

How are we addressing any additional CSSF information requests? Are we prepared for any potential ESG site inspections?

4

Have we identified how many data points we must collect to comply with our ESG disclosure requirements?

By

Aude Payan

Director, ESG & Regulatory Risk
E: aude.payan@kpmg.lu

Julie Castiaux

Partner, Sustainability Lead
E: julie.castiaux@kpmg.lu

From AML to anti-tax crime laundering: can you manage your tax risks?

When the scope of AML widens to tax crime, compliance officers need to hit the tax books. And when the financial regulator also comes into play, the topic is a must for the boardroom.

Over the past few years, the international tax landscape has shifted toward increasing tax transparency and enhancing tax conformity across many industries and professions. As a result, Luxembourg underwent a significant tax reform in 2017, which extended the criminal offense of money laundering to include aggravated tax fraud (fraude fiscale aggravée) and tax evasion (escroquerie fiscale).

CSSF Circular 17/650 (the “Circular”), drafted jointly with the Financial Intelligence Unit (FIU) and the CSSF, clarified the practical application of these new provisions and provided a list of 21 indicators for CSSF-supervised firms, including the banking sector. These indicators are generally concerned with transparency, substance and transactions.

The Circular requires banks to implement policies and procedures to evaluate customers from a tax perspective and identify certain tax-related risks. They must also provide sufficient training to AML and KYC staff members to ensure the 21 indicators are effectively implemented.

If tax risks remain even after a bank has applied specific mitigation measures, they must report them to the FIU.

What are the risks of non-compliance?

If banks do not integrate the Circular’s tax indicators into their internal procedures, they may be considered non-compliant with their AML obligations.

In case of a breach, the CSSF could impose (public) administrative sanctions, ranging from a warning or an administrative fine up to withdrawing or suspending a bank’s registration or authorization. In a worst-case scenario, banks may be considered a money laundering accomplice, resulting in criminal fines and up to five years of imprisonment.

Questions that may be raised

1

Are we directly supervised by the CSSF?

4

Have we properly implemented the Circular's requirements in our procedures and policies?

2

Have we performed an impact assessment of the Circular on our business?

5

How robust is our oversight of third-party delegates and service providers?

3

If yes, have we implemented the necessary mitigation measures to address all identified issues?

6

Has the CSSF already requested an AML/CFT on-site inspection? Are we prepared for such an inspection?

By

Daniel Rech

Tax Partner, Banking Leader

E: daniel.rech@kpmg.lu

Digital transformation in banking

Unite your enterprise to help optimize costs and improve CX

Many banks operate a patchwork of legacy systems and applications - business processes often require workarounds, while customer-facing channels are loosely linked but not fully integrated. As a result, it can be challenging to keep pace with fast-changing customer expectations. All the while, bank executives are facing enormous pressure to reduce costs and drive profitability.

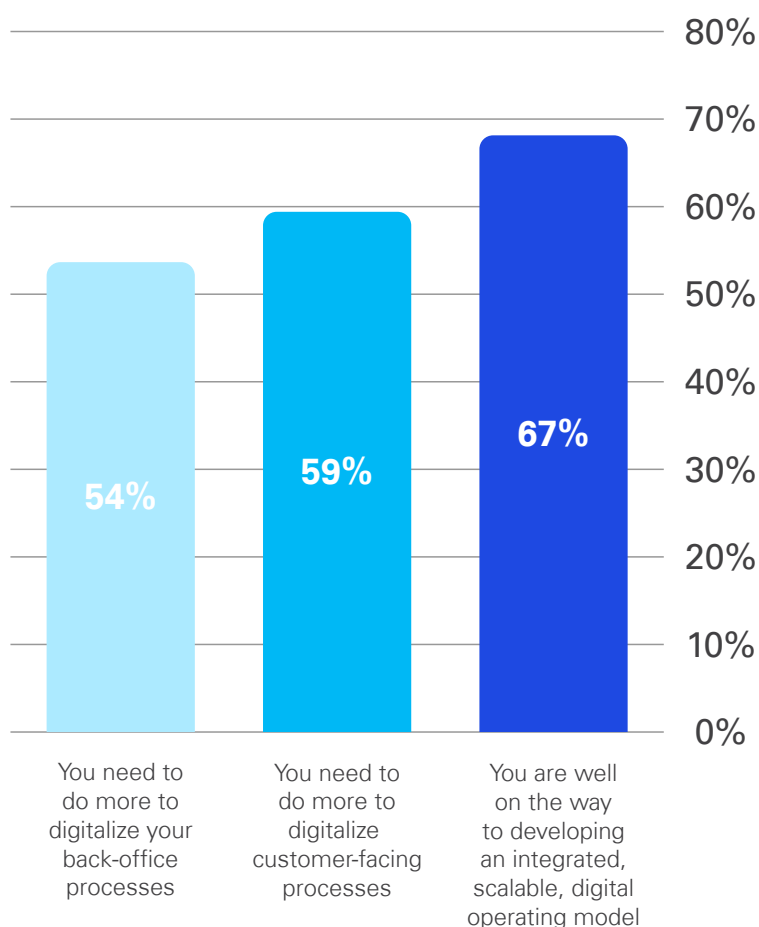
Maintaining outdated, disjointed IT systems is a significant drag on efficiency and operational agility. Modernizing IT systems through well-designed, planned and executed digital transformation projects can solve a myriad of problems at once.

Banks have accepted that digitalization is no longer a nice-to-have. It's now essential to customer and collaborator experiences, and crucial for cost reduction.

In 2024, a KPMG survey of senior banking executives found that investment in digital innovation and technology implementation continues despite the economic environment (Figure 1)³.

While many bank executives are focused on creating integrated, scalable digital operating models, our findings reveal there's still significant work to be done regarding customer-facing and back-office initiatives.

Figure1 : Where are you on your digitilization/ transformation journey?



³ KPMG, [Luxembourg banking insights 2024](#), 2024

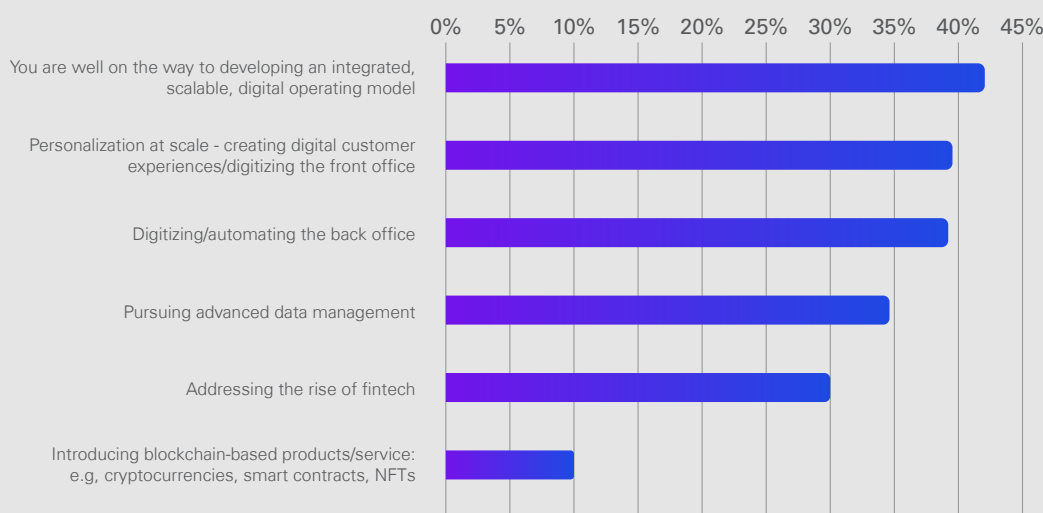
Cost of inaction: too high?

Ninety-seven percent of respondents stated that in the next fiscal year, digitalization efforts would either proceed as planned or simply slow down. Only 6% said they would stop altogether.

Banks are primarily focused on migrating substantial processes to the cloud. They are leveraging advanced analytics, including AI and machine learning, and taking steps to continue replacing core banking technologies. In addition, banks have or are starting to make significant technology investments to enhance CX and build digital capabilities.

In Luxembourg, banks prioritize digitalization to enhance products, automate processes, ensure compliance and improve customer satisfaction (Figure 2). This aligns with broader market strategies, suggesting that banks view digitalization as a key lever to achieve their strategic objectives.

Figure2 : What are your organization's main digitalization goals?

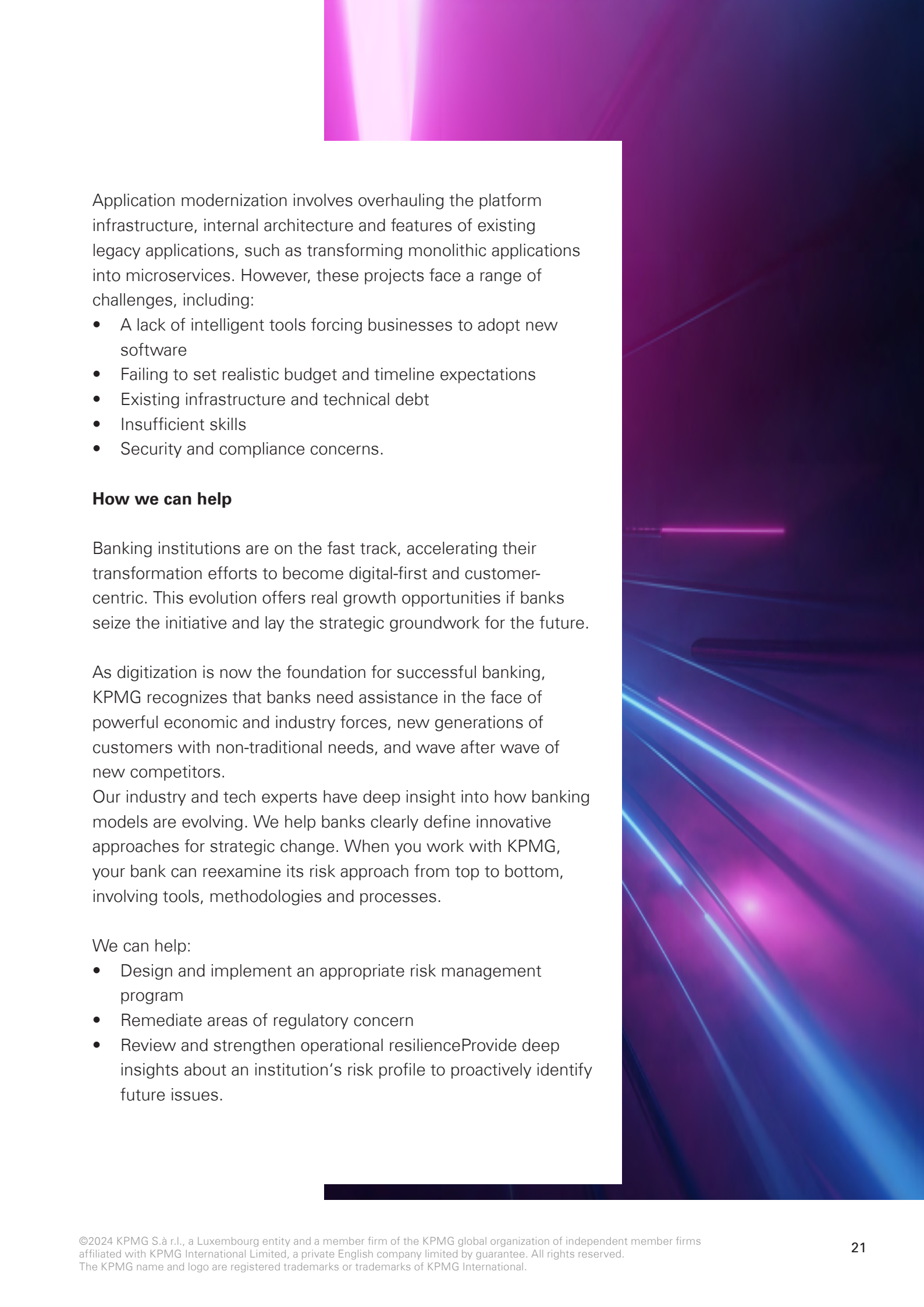


In the coming months, we expect banks to expand their efforts around digitalizing foundational elements to realize meaningful and measurable return on investment (ROI). They will also pay significant attention to cloud and app modernizations to fuel product innovation, enable real-time processing, and address an array of growing customer needs.

Cloud and app modernizations: a recipe for successful digital transformations?

While the cloud has enabled and championed digital transformation and modernization in many organizations, banks must look beyond the traditional “lift and shift” migrations. Instead, they should leverage cloud-native architectures like containers and microservices to:

- Enjoy a faster time to market
- Handle scalability and agility challenges
- Generate business value
- Harness intelligent automation to create exceptional CX.



Application modernization involves overhauling the platform infrastructure, internal architecture and features of existing legacy applications, such as transforming monolithic applications into microservices. However, these projects face a range of challenges, including:

- A lack of intelligent tools forcing businesses to adopt new software
- Failing to set realistic budget and timeline expectations
- Existing infrastructure and technical debt
- Insufficient skills
- Security and compliance concerns.

How we can help

Banking institutions are on the fast track, accelerating their transformation efforts to become digital-first and customer-centric. This evolution offers real growth opportunities if banks seize the initiative and lay the strategic groundwork for the future.

As digitization is now the foundation for successful banking, KPMG recognizes that banks need assistance in the face of powerful economic and industry forces, new generations of customers with non-traditional needs, and wave after wave of new competitors.

Our industry and tech experts have deep insight into how banking models are evolving. We help banks clearly define innovative approaches for strategic change. When you work with KPMG, your bank can reexamine its risk approach from top to bottom, involving tools, methodologies and processes.

We can help:

- Design and implement an appropriate risk management program
- Remediate areas of regulatory concern
- Review and strengthen operational resilienceProvide deep insights about an institution's risk profile to proactively identify future issues.

Questions that may be raised

1

Which steps must we take before moving to the cloud?

3

How can we stop working in silos?

2

Which frameworks will we need to use across all aspects of our digital transformation?

4

How can we quickly upskill our multigenerational workforce?

By

Xavier Roch Lhotellier

Partner

E: xavier.rochlhotellier@kpmg.lu

From open banking to open finance

The shift from open banking to open finance marks a significant advancement in the financial services sector, broadening the scope of data sharing and integration beyond traditional banking services.

Initiated under the second Payment Services Directive (PSD2) in 2018, open banking aims to enhance competition, drive innovation and deliver superior financial services to consumers. Banks were mandated to provide third-party providers access to payment services and customer data through application programming interfaces (APIs). This move facilitated account aggregation and payment initiation, as well as the development of more personalized financial products.

Building on open banking's foundations, open finance is expanding data sharing to a wider array of financial products and services, including savings, investments, insurance and pensions. This evolution aims to create a more integrated and comprehensive financial ecosystem.

But which regulations are guiding this transition and must be observed to successfully navigate these changing market conditions?

Game changer texts for the payments landscape, in a nutshell

In the rapidly evolving landscape of European finance, four texts are key to the future of transactions and digital banking. Together, they are poised to shape the dynamics of the financial landscape, ensuring greater transparency, accessibility and innovation for consumers and businesses alike.

1. The **third Payment Services Directive (PSD3)** is the latest iteration of the directive regulating the EU's payment services. It expands on PSD1 and PSD2 to further enhance consumer protection, promote innovation, and improve the security of online payments. The text is currently under review, with its final version expected to be published in late 2024 or early 2025.
2. The **Payment Services Regulation (PSR)** is designed to oversee the operation of payment systems within a given jurisdiction. It aims to ensure that payment services are transparent and competitive in nature. The rules cover aspects like access to payment systems, pricing, and the general conduct of payment service providers (PSPs). As with PSD3, the PSR proposal is under review and should be published in late 2024 or early 2025.
3. The **Financial Data Access Regulation (FIDA)** promotes the financial sector's competition and innovation by making it easier for new market entrants to offer new products and services. It will also give consumers more control over their financial data and ease switching to other providers. Since the legislative process is still at an early stage, FIDA is expected to be implemented in 2026 at the earliest.
4. The **Instant Payments Regulation (IPR)** aims to increase the uptake of euro instant credit transfers and make euro instant payments (IPs) universally available and affordable to EU consumers and businesses, increasing trust and removing friction as a result. Following its adoption and official publication in March 2024, the IPR will come into effect after a transition period.

These European rules promote competition between banks and FinTechs, diversifying payment solutions and boosting European-led innovation. We take a deep dive into these game-changer texts, considering their scope, key points, nature and expected go-live dates.

PSD3 and PSR: two complementary texts bolstering open banking

As technological advancements continue to shape the financial landscape, the EU's regulatory framework must adapt to ensure secure, efficient and competitive financial markets. The PSD3 and the PSR represent the EU's commitment to fostering an innovative financial ecosystem while addressing the PSD2's shortcomings.

Furthermore, PSD3 and PSR will integrate features of the E-Money Directive (EMD) to also mandate rules for EU electronic institutions, abolishing the EMD as a result.

	PSD3	PSR
SCOPE	Aims to further enhance consumer protection, promote the payment industry's innovation, and improve the security of internet payments and account access within the EU.	Provides legal guidelines for EU electronic payments, promoting competition and innovation by requiring banks to share API-accessible, user-approved data.
KEY POINTS	<ul style="list-style-type: none">• Improves consumer protection by increasing consumer rights and information about fees, and limiting customer liability in case of unauthorized payments.• Boosts consumer security by emphasizing strong customer authentication and security measures, ensuring electronic payments are safe and secure• Enhances data access by promoting open banking, allowing third-party providers to access bank data to offer innovative financial services.	<ul style="list-style-type: none">• Enhances open banking competitiveness by promoting competition and innovation in payment systems, ensuring they are operated and used in a way that considers the interest of all users.• Levels the playing field between banks and PSPs by ensuring payment systems are accessible to a wide range of PSPs.• Strengthens enforcement possibilities by offering mechanisms to resolve disputes between PSPs and payment systems.
NATURE	EU Directive:	EU Regulation:
	<ul style="list-style-type: none">• EU countries must transpose the rules into their national laws.• EU countries have leeway in how they implement it.	<ul style="list-style-type: none">• Once adopted and entered into force, it applies directly to EU Member States.• Therefore, it does not need to be transposed into national laws.
EXPECTED GO LIVE	<ul style="list-style-type: none">• 2024 earliest: PSD3 adoption.• 2026 earliest: PSD3 implementation.	<ul style="list-style-type: none">• 2024 earliest: PSR adoption.• 2026 earliest: PSR implementation.

FIDA and IPR: key steps towards open finance

FIDA and IPR complete the EU's endeavor for a comprehensive and consistent regulatory framework, underlining its ambition to further drive the open finance transition. Accordingly, the recently published IPR and upcoming FIDA texts guide the future development of an innovative financial landscape.

	FIDA	IPR
SCOPE	Introduces "open finance" by broadening the scope of customer data that can be shared, opening the door to new types of business models for financial institutions. It covers nearly all financial services data.	Focuses on instant credit transfers in euro and improves the availability of IP options to consumers and businesses in EU and EEA countries.
KEY POINTS	<ul style="list-style-type: none"> • Enhances open banking competitiveness: grants consumers and small and medium-sized enterprises (SMEs) the right to authorize third parties (or data users) to access their data held by financial institutions (or data holders). • Improves data access: data holders will be able to ask for reasonable compensation for making data accessible to data users. • Enhances consumer protection: data users will have "read access" but will not be able to initiate transactions on behalf of customers. 	<ul style="list-style-type: none"> • Improves the strategic autonomy of the European economic and financial sector: the new rules will help reduce any excessive reliance on third-country financial institutions and infrastructures. • Increases the possibilities to mobilize cash-flows: IPs allow people to transfer money within 10 seconds at any time of the day, including outside business hours, not only within the same country but also to another EU Member State. • Improves access and transparency of payments: EU PSPs will have to meet specific requirements, such as making IPs universally available and affordable.
NATURE	EU Regulation: <ul style="list-style-type: none"> • Once adopted and entered into force, it applies directly to EU Member States. • Therefore, it does not need to be transposed into national laws. 	
EXPECTED GO LIVE	<ul style="list-style-type: none"> • 2024 earliest: FIDA adoption. • 2026 earliest: FIDA implementation. 	<ul style="list-style-type: none"> • 13 and 19 March 2024: IPR adoption and legislation. • 8 April 2024: Entry into force. • The IPR's requirements have different deadlines, but a first set of obligations for PSPs will have to be complied with as of 9 January 2025.

The shift from open banking to open finance will significantly broaden the scope of data sharing, delivering both new challenges and business opportunities. While firms will be able to provide more personalized and comprehensive services to their customers, they must also ensure robust data management and security measures as well as regulatory compliance.

To help firms benefit from this transition and realize new value creation potentials, KPMG combines regulatory and strategic experience to offer holistic and future-oriented advisory services.

Questions that may be raised

1

What are the IPR's specific requirements and deadlines? For example, will our clients be able to receive IPs by 9 January 2025 and send IPs by 9 October 2025?

4

How can we ensure the security and fraud prevention measures for IPs?

2

What are the (technical) implications of adapting to these new requirements? For example, are our current systems and infrastructures capable of processing IPs or is external support required?

5

How can we comply with uniform standards for data access and sharing under FIDA, and which technological adjustments may be necessary?

3

Have the first and second lines of defense come together to amend the bank's AML framework to reflect the challenges of IPs?

6

How can we leverage the FIDA's opportunities to enhance customer experience and innovation?

By

Thor-Hagen Scheller

Director, Advisory

E: thor-hagen.scheller@kpmg.lu

Elevating CX: a strategic priority for banking in 2025

Why?

To tackle the rapidly changing landscape of the next 12 months, CX is a critical differentiator for private, retail, and corporate banks. Evolving competition, regulatory pressures and customer expectations drive banks to prioritize CX to build trust, enhance loyalty and drive sustainable growth.

The number one rule: customer service, customer service and customer service

While banking services' digitalization accelerated during the COVID-19 pandemic, the number of Luxembourg banking agents has decreased by 30% since 2018, following a general trend in Europe⁴. The result is increasingly frustrated clients who struggle to access services or obtain answers to their questions.

Clients' uncertainty for the future, nurtured by several turbulent years, has made human-to-human contact a must in customer service. Some banks have expanded their contact center workforces or reopened more agency timeslots without appointment to meet their customers' demands.

Finding the ideal phygital balance in delivered CX is key to managing a bank's transformation priorities and related investments that serve both the institution and its clients' interests.

In today's highly competitive market, customer service has evolved into a powerful sales driver. Personalized, empathetic and efficient service builds trust and fosters loyalty, turning satisfied customers into repeat buyers and brand advocates.

When customer service teams resolve issues swiftly and exceed expectations, they create positive experiences that not only boost customer retention but also generate referrals and upsell opportunities.

In the banking industry where trust and relationships are paramount, exceptional customer service often directly generates new business, making it as crucial as traditional sales efforts in driving revenue growth.



There are
30%
fewer agencies in the
luxembourg territory
since 2018³

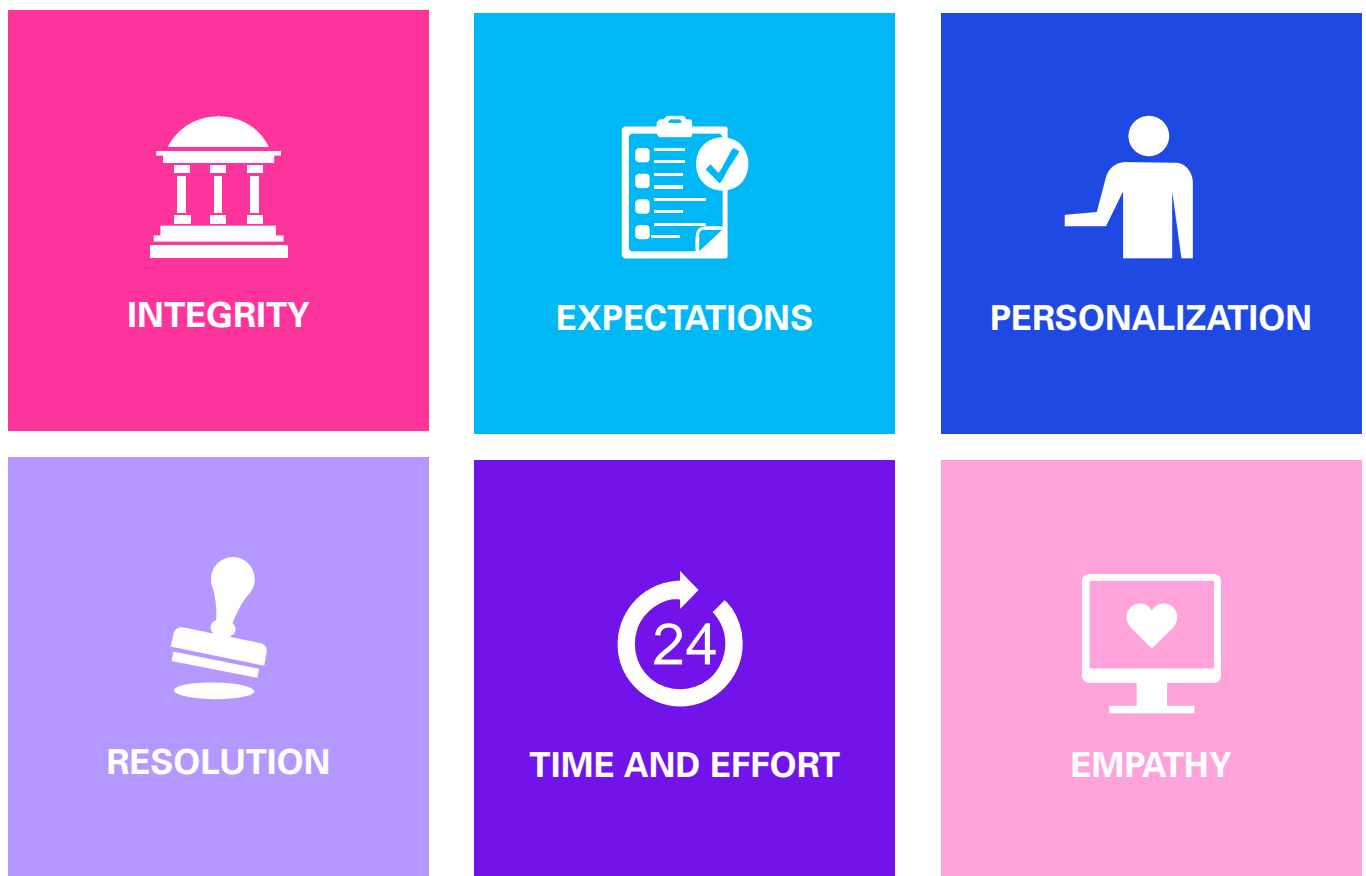
³ KPMG, [Luxembourg banking insights 2024](#), 2024

⁴ ABBL, [Annual Report 2023](#), 2024

What?

The six pillars of CX excellence

The essential characteristics of strong CX are integrity, expectations, personalization, resolution, time and effort, and empathy. Whether resulting in an increased share of wallet, loyalty or advocacy, these six factors are the prerequisites for commercial success and drive sustainable growth.



Integrity: a foundation across all banking segments

Trust remains banks' universal currency, but its foundations can vary.

In private banking, trust is often built on discretion, confidentiality and consistently delivering superior financial outcomes. Clients expect transparency across fee structures, investment strategies and risk management processes to maintain their confidence.

On the other hand, retail banking clients can place a greater emphasis on reliability and security. They expect their bank to protect their assets, ensure their transactions' security, and communicate clearly and honestly. Social responsibility and ethical practices are also increasingly important in building trust with retail customers.

Meeting and exceeding expectations: differentiating in a competitive market

As customer expectations evolve rapidly, banks must keep their fingers on the pulse to maintain a competitive edge.

Nowadays, clients expect seamless digital experiences, from intuitive mobile apps to efficient online loan applications. The ability to manage finances anytime and anywhere is paramount, and banks meeting these expectations with innovative, robust and user-friendly platforms will stand out.

However, banks must listen to all customer categories to avoid pursuing a single, fully digital direction that alienates clients who trust human relationships above all.

Personalization: catering to diverse banking needs

While personalization is increasingly essential across all banking segments, the approach differs according to clients' specific needs. As private banking clients expect bespoke services, personalization means tailoring wealth management and investment strategies to align with individual financial goals, risk tolerance and even personal values. This high-touch approach is crucial for building long-term relationships with high-net-worth individuals (HNWIs).

For mass retail clients, banks are challenged to offer personalized experiences at scale, creating customized product recommendations and targeted offers that resonate with their broad customer base. By analyzing spending patterns, financial behavior and life stages, banks can deliver relevant, timely advice that enhances the everyday banking experience.

Resolution: turning problems into opportunities

Whether the problem is related to investment performance, service errors or financial disputes, the ability to address concerns quickly and satisfactorily is essential for maintaining trust.

Banks providing immediate support through digital channels, such as chatbots or mobile apps, can significantly enhance their CX by resolving issues promptly.

The stakes are often high for corporate clients, whether it's a significant transaction delay or a credit facility issue. Specialized teams are necessary to address and resolve complex problems swiftly, transforming potential disruptions into opportunities to reinforce trust and loyalty.

Time and effort: simplifying the banking experience.

Clients expect streamlined processes and services that minimize the time they spend on financial management, whether accessing accounts, executing investment decisions or consulting with advisors.

Time is money, and clients expect banking services that enable them to complete financial tasks quickly and with minimal friction.

Simplifying everyday transactions, such as mobile deposits, bill payments and fund transfers, reduces the time and effort required to manage finances. While intuitive digital interfaces and automated processes can help deliver a seamless banking experience.

Empathy: understanding and responding to client needs

When we talk about CX, empathy is often the first quality that comes to mind. In banking, it involves understanding and responding to a client's unique challenges and concerns. This can't be achieved without taking the time to listen to clients.

Empathy means recognizing the personal and emotional aspects of wealth management, including life events, family dynamics or philanthropic desires. It's also appreciated when clients face financial difficulties, such as unexpected expenses, unemployment or credit issues. Banks that offer flexible solutions like loan modifications or demonstrate a commitment to their customers' well-being are more likely to retain their client base.

How?

Good CX doesn't happen by accident. It must be managed.

Following the success of the 2021 Customer Experience Excellence Report, KPMG Luxembourg embarked on a new, unique study to understand how organizations are internally managing their CX: *the Customer Experience Management Maturity Assessment 2023–24* ⁵.

The study evaluated the five domains of CX management, or CXM.

1

CX strategy

The ability to implement, communicate and involve collaborators in the CX strategy to achieve the organization's CX goals.

2

Customer insights and understanding

The ability to collect, harness and understand customer data to turn it into actionable insights.

3

Metrics, measurement and ROI

The ability to define, measure and monitor CX metrics to inform business decisions.

4

Design, implementation and innovation

The ability to improve and develop CX initiatives and solutions to engage customers and drive business performance.

5

Culture and accountability

The ability to build a customer-centric organization and culture that inspires people to deliver on the customer promise.

⁵ KPMG, [Customer Experience Management Maturity Assessment 2023-24](#), 2024

How intentional is the delivered experience?

Although the banking industry seems ahead of other sectors in terms of CX, significant improvement is still required across all domains.

While Luxembourg organizations often declare that client-centricity is important, our study found there isn't always a proper governance in place to manage it. In other words, there's a gap between their intentions and their actions.

A declaration of intent to put the client at the center of the bank's activities is insufficient; it's also necessary to articulate a CX governance that relies on a robust strategy. This involves incorporating the bank's CX vision into a concrete and clear action plan that defines measurable objectives and tangible results.

AI or not AI? That's the question

The survey's interviews with Luxembourg banks uncovered that the sector's AI adoption is uneven.

Most participating banks declared they are considering AI to streamline operations and automate back-office tasks. On the other hand, using AI to interact directly with customers through large language models (LLMs) has yet to reach its full potential.



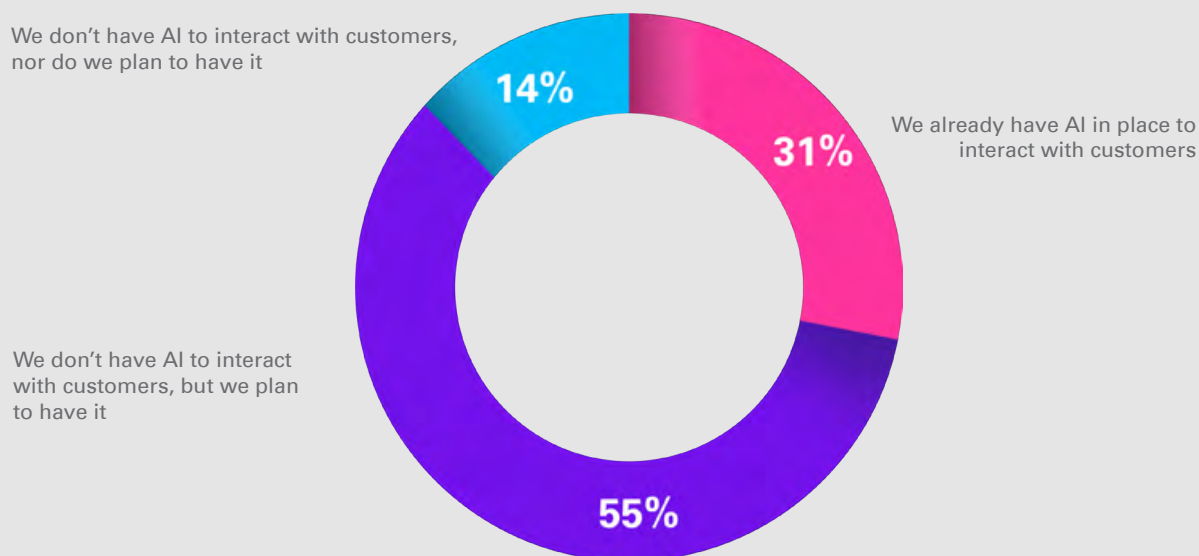
**While most organizations
believe they meet
or go beyond their customers'
expectations, only**

59%

**follow CX key metrics to
demonstrate this⁶.**

⁶ KPMG, [Customer Experience Management Maturity Assessment 2023-24](#), 2024

Figure3: Do you use or do you plan to use AI to interact with your clients?⁷



Notably, 14% of the interviewees don't plan to leverage AI to interact with their clients (Figure 3).

According to KPMG's 2023 global Trust in artificial intelligence report, three in five (61%) respondents were wary about trusting AI systems, indicating there's more work to be done for consumers and organizations alike to increase trust in AI⁸.

Clients expect transparency and want to know if and why banks are using AI.

To go further...

Align your business to meet your customers' needs and create a seamless, agile and digitally enabled organization that delivers leading experiences and new levels of performance and value.

Get to know [KPMG Connected Enterprise](#), KPMG's customer centric, agile approach to digital transformation, tailored by sector.

Contact us and request your Customer Experience Management Maturity Assessment.

By
Julien Hugo
Director, Customer advisory
E: julien.hugo@kpmg.lu

⁷ KPMG, [Customer Experience Management Maturity Assessment 2023-24](#), 2024

⁸ KPMG, [Trust in artificial intelligence: 2023 global study on the shifting public perceptions of AI](#), 2023

CRR III and CRD VI

On 19 June 2024, the European Parliament and the Council published the new Banking Package in the Official Journal of the European Union, which comprises:

- The third Capital Requirements Regulation (CRR III), introducing amendments to requirements for credit risk, credit valuation adjustment (CVA) risk, operational risk, market risk and the output floor.
- The sixth Capital Requirements Directive (CRD VI), introducing amendments to supervisory powers, sanctions, third-country branches (TCBs), and ESG risks.

The new Banking Package transposes the final reforms of the Basel III framework, with the primary goals of:



Strengthening the risk based capital framework



Integrating ESG-risk focus into the prudential framework



Harmonizing supervisory powers and tools



Improving access to institutions' prudential data

The new Banking Package entered into force on **9 July 2024** and CRR III and CRD VI **will apply from 1 January 2025**.

EBA next steps

In addition to the Banking Package, the European Banking Authority (**EBA**) is **mandated** to publish about **140 additional documents**, including RTS and ITS, guidelines, opinions, reports, national lists and registers. The authority has published **a four-phase roadmap** to achieve these goals.

<h2>Phase 1:</h2> <p>Deadline: 9 July 2025</p> <p>Includes 32 mandates covering credit, market and operational risk, and the first CRD mandates regarding ESG.</p>	<h2>Phase 2:</h2> <p>Deadline: 9 July 2026</p> <p>Includes 43 mandates regarding credit, operational and market risk, as well as those related to high EU standards regarding governance and TBCs' access to the single market.</p>
<h2>Phase 3:</h2> <p>Deadline: 9 July 2027</p> <p>Includes 21 mandates regarding regulatory products as well as several reports. In this third phase, most of the technical standards and guidelines will be closed.</p>	<h2>Phase 4:</h2> <p>Deadline: 9 July 2028</p> <p>Includes 36 mandates of mostly reports, providing information about the implementation progress, results and challenges.</p>
<h2>Ongoing:</h2> <p>Seven other ongoing and reoccurring mandates outside of the four phases will be made operational on 9 July 2025.</p>	

Overview of key CRR/II changes

	Main changes	What to do next
Credit risk: standardized approach for counterparty credit risk (SA-CR)	<ul style="list-style-type: none"> No longer possible to use country ratings for unrated institutions, which will follow a new grading system Due diligence required on the external credit ratings used New exposure classes, classified today under corporates Other changes to risk-weights and credit conversion factors (CCFs). 	<ul style="list-style-type: none"> Calculate the impact on the credit risk capital requirements and adjust calculation and reporting tools Re-assess the risk-adjusted profitability and pricing of the impacted products Potentially revise interbank and/or treasury frameworks to minimize the impacts on capital Potentially review and reduce contracts of unconditionally cancellable commitments Set up processes to meet the due diligence requirements together with your group.
Credit risk: internal ratings based approach (IRBA)	<ul style="list-style-type: none"> Stronger limitation of the IRBA scope New input floors for loss given default (LGD) and CCFs 	<ul style="list-style-type: none"> Assess the relevance of keeping IRB models on concerned portfolios Modify the relevant and new input floors for LGD and the probability of default (PD) cap in the calculation tool.
Credit risk mitigation techniques	<ul style="list-style-type: none"> Revised eligibility criteria and haircuts for financial collateral Revised values of secured LGDs and collateral haircuts 	<ul style="list-style-type: none"> Calculate the impact on the credit risk capital requirements and integrate the new criteria in the calculation and reporting tool Potentially revise credit granting and collateral monitoring processes and adjust clients' collateral acceptance policy, if relevant.
Operational risk	<ul style="list-style-type: none"> Replaces existing approaches with a single, non-model-based approach Models will still be used for the internal capital adequacy assessment process (ICAAP) 	<ul style="list-style-type: none"> Calculate the impact on the operational risk capital requirements and include the new calculation method in the reporting tool, considering the business' complete volume and size (e.g. including results from expenses and any contribution to net trading losses) Ensure 10-year incident losses are available and included in the calculation tool.
Market risk	<ul style="list-style-type: none"> New trading book definition Introduces a new calculation approach depending on the size of the trading book 	<ul style="list-style-type: none"> Assess the impact of the new trading book definition on the business model Review and verify the relevance of the classification of products to the trading or banking book Include the new calculation method in the reporting tool.
CVA risk	Introduces three new approaches: the standardized approach, basic approach and simplified approach	<ul style="list-style-type: none"> Implement the required infrastructure and models to calculate CVA risk capital according to the selected approach Assess capital requirements under the new regime and the products in scope to be considered
Output floor	Lowens the boundary for capital requirements produced by institutions' internal models (up to 72.5%)	<ul style="list-style-type: none"> Assess the relevance of keeping internal models on some portfolios Assess the cost of maintaining both internal and standardized models Implement and test the standardized approaches in the reporting tool.
Sustainability	ESG risks must be implemented into strategy, processes and policies to ensure their identification, measurement, management and monitoring	<ul style="list-style-type: none"> Ensure ESG risk is properly integrated into the risk management framework Ensure ESG risk controls are embedded in the internal audit framework.

What does CRD VI bring?

- **Sets detailed requirements for banks to manage and disclose ESG risks**, particularly climate-related ones. Processes should be implemented to identify, manage, monitor and report ESG risks over the short, medium and long term.
- **Imposes stricter governance and accountability on banks' management bodies** to manage and steer the institution's financial results and risk exposures, including the management body's selection process and fit-and-proper rules.
- **Grants supervisors expanded authority to address risks**, including ESG, and to intervene earlier in distressed banks.
- **Introduces crypto assets into the risk management framework** by imposing dedicated governance and risk management processes regarding crypto assets.
- **Harmonizes TCB supervision** by imposing more consistent regulation and supervision of TCBs operating in the EU.

CRD VI also delivers stricter systemic risk buffers for systemically important institutions and more frequent countercyclical buffers to be considered in banks' capital requirements. In addition, it provides more guidance and requirements on integrating ESG and other emerging risks into stress testing and capital planning.

Overall, the new Banking Package strengthens institutions' internal governance, risk culture and capital requirements. While CRR III has stricter capital requirements than its predecessor, CRD VI aims to build a risk-aware culture and a strong oversight of risk management by management bodies to ensure banks continue to adapt to the sector's continuously evolving risks.



Questions that may be raised

1

Have we assessed the impact of the changes on our key capital ratios, and are we ready to calculate and report under the new requirements? Are our systems and controls effectively operating to reflect the changes?

2

Do all the changes have a fairly flat impact on our Pillar 1 and 2 capital requirements, or will we have significantly higher capital requirements that we need to allocate?

3

Are our processes up to date and tested? Is the management body accountable for the required changes and ready to face regulatory interventions? Or do we need help to prioritize our best course of action depending on the impact on our capital ratios and processes?

By

Alix Tchana

Partner

E: alix.tchana@kpmg.lu

Aude Payan

Director, ESG & Regulatory Risk

E: aude.payan@kpmg.lu

Markets in Crypto-Assets (MiCA) Regulation

The MiCA Regulation, part of the EU Digital Finance Package, promotes uniform market rules for crypto assets across the EU. Bolstered by a set of RTS, MiCA establishes the EU's first comprehensive framework for issuing, offering and admitting crypto assets to trading, while also protecting consumers and providing legal certainty and financial stability.

MiCA enables the passporting of crypto-asset services across EU Member States, allowing both traditional institutions and new players to take part in this emerging market. It will fully apply as of 30 December 2024, although its rules for issuers of asset-referenced tokens (ARTs) and e-money tokens (EMTs) have applied since 30 June 2024.

Categorization of crypto assets

MiCA defines three types of crypto assets, which are subject to different requirements depending on their associated risks:

1. EMTs, which maintain a stable value by mirroring an official currency.
2. ARTs, which maintain a stable value through one or several underlying liquid asset(s).
3. Crypto assets that are not considered ARTs or EMTs, a catch-all category that includes utility tokens and fungible tokens issued by a legal person.

Non-fungible tokens (NFTs) and assets that provide access to goods or services, work with a limited network of merchants, or have no identifiable user remain out of scope of MiCA.

Crypto-asset services

Under MiCA, credit institutions established in the EU can provide the following services:

- Providing crypto-asset custody and administration on behalf of clients
- Operating a crypto-asset trading platform
- Exchanging crypto assets for funds or other crypto assets
- Executing crypto-asset orders on behalf of clients
- Placing crypto asset orders
- Receiving and transmitting crypto-asset orders on behalf of clients
- Providing crypto-asset advice
- Providing crypto-asset portfolio management
- Providing crypto-asset transfer services on behalf of clients.

To become authorized as a crypto-asset service provider (CASP), credit institutions need to notify their competent authority at least 40 days before the date they plan to provide these crypto-asset services. This includes a detailed business case, including:

- A risk-benefit assessment
- The required adaptations to their governance and risk management frameworks
- The effective handling of counterparty and concentration risk
- The implementation of investor protection rules.

Accounting and capital requirements

Credit institutions wanting to provide crypto-asset services must adhere to several accounting and capital rules.

1. When risk-weighting crypto assets under the CRR, gross exposures to virtual assets should receive a 1,250% risk weight or be deducted from capital.
2. Crypto assets should be considered as intangible for accounting purposes, unless they qualify for the accounting treatment of cash equivalents or financial instruments.
3. The institution's authorized management must carefully assess, document and validate its accounting approach shall be carefully assessed, documented, and validated by the institution's authorized management, as well as the recognition of netting effects or the classification as cash or financial instruments.

Credit institutions can open accounts that allow customers to deposit crypto assets comparable to securities accounts to safekeep traditional financial instruments. These must be segregated from the bank's own assets.

The CSSF expects credit institutions facilitating crypto-asset investment to establish an effective investor protection framework.

Questions that may be raised

1

Is there a client demand for any crypto-asset services that we can provide?

3

Have we assessed the accounting implications that may be involved?

2

Do we meet the necessary capital requirements to provide crypto-asset services?

4

Have we considered any AML/CFT and market abuse implications?

By

Thor-Hagen Scheller

Director, Advisory

E: thor-hagen.scheller@kpmg.lu

New investment tax credit

On 19 December 2023, the Luxembourg Parliament approved bill n° 8276, overhauling the investment tax credit (ITC) regime that taxpayers could claim against their corporate income tax. This new regime, which took effect on 1 January 2024, increases the tax incentive for eligible projects in digital transformation or ecological and energy transition.

Background

Under the old regime, companies could benefit from two types of ITCs under Article 152bis of the Luxembourg Income Tax Law (LITL):

- A tax credit for “global investment” in specified property of:
 - Eight percent of the qualifying assets’ total acquisition price up to the first €150,000
 - Two percent for the portion exceeding €150,000.
- A 13% tax credit on the “additional investment” in qualifying depreciable tangible assets in a given year.

On 13 July 2023, Bill n° 8276 was introduced to reshape the previous ITC regime for companies.

Alongside increasing the existing global ITC rate from 8% to 12%, the new regime creates a new ITC incentive for Luxembourg businesses’ investments in their digital transformation or ecological and energy transition, as well as related expenses.

The new regime defines digital transformation and ecological and energy transition as follows:

Digital transformation

Achieving a process or organizational innovation by implementing and using digital technologies, such as:

- Redefining production processes to increase productivity or resource efficiency
- Implementing an innovative business model to create new value for stakeholders
- Significantly redefining the delivery of services to create new value for stakeholders
- Modernizing the company’s organization to create new value for stakeholders
- Improving digital security.

Ecological and energy

Defined as “any change that reduces the environmental impact of the production or consumption of energy or the use of resources”, such as:

- Improving a production process’ energy efficiency, and/or material efficiency and/or significantly reducing its carbon emissions
- Enabling the self-consumption of produced energy or the storing of energy from renewable, non-fossil sources
- Reducing air pollution from production sites
- Promoting the extension of products through re-use.

New regime overview

New ITC of 18% for investments

- In digital transformation or ecological and energy transition projects
- Includes not only investments but also operating expenses (e.g. personal expenses and third-party costs)

18%

New tax relief for investments in digital transformation or ecological and energy transition

12% of global investment

- Increases the global investment tax relief rate from 8% to 12%
- Abolishes the previous €150,000 investment tranche

Increase to

12%

for global ITC

14% for investments qualifying for Article 32bis LITL

- Covers tangible depreciable assets with special amortization
- For example, investments in assets to reduce water use; eliminate or reduce water, air or noise pollution; and reduce waste

14%

for investments qualifying for Article 32bis LITL energy transition

6% or 18% for investments in tangible depreciable assets and software

- 6% if these assets are expected to benefit from the 12% global investment tax credit
- Otherwise, the tax relief is 18%

6/18%

for investments in tangible depreciable assets and software transition

ITC 18%: new attestation and certification process

1. Eligibility attestation

The financial institution files an eligibility application with the Ministry of Economy, which includes the following information about the project, among others:

- Name, location and description
- Objective, including a justification of how this objective will be met
- Start and end dates.

Only investments made and operating expenses incurred after the application is submitted are covered. The Ministry of Economy will grant or refuse the application within three months of receipt.

2. Annual certificate

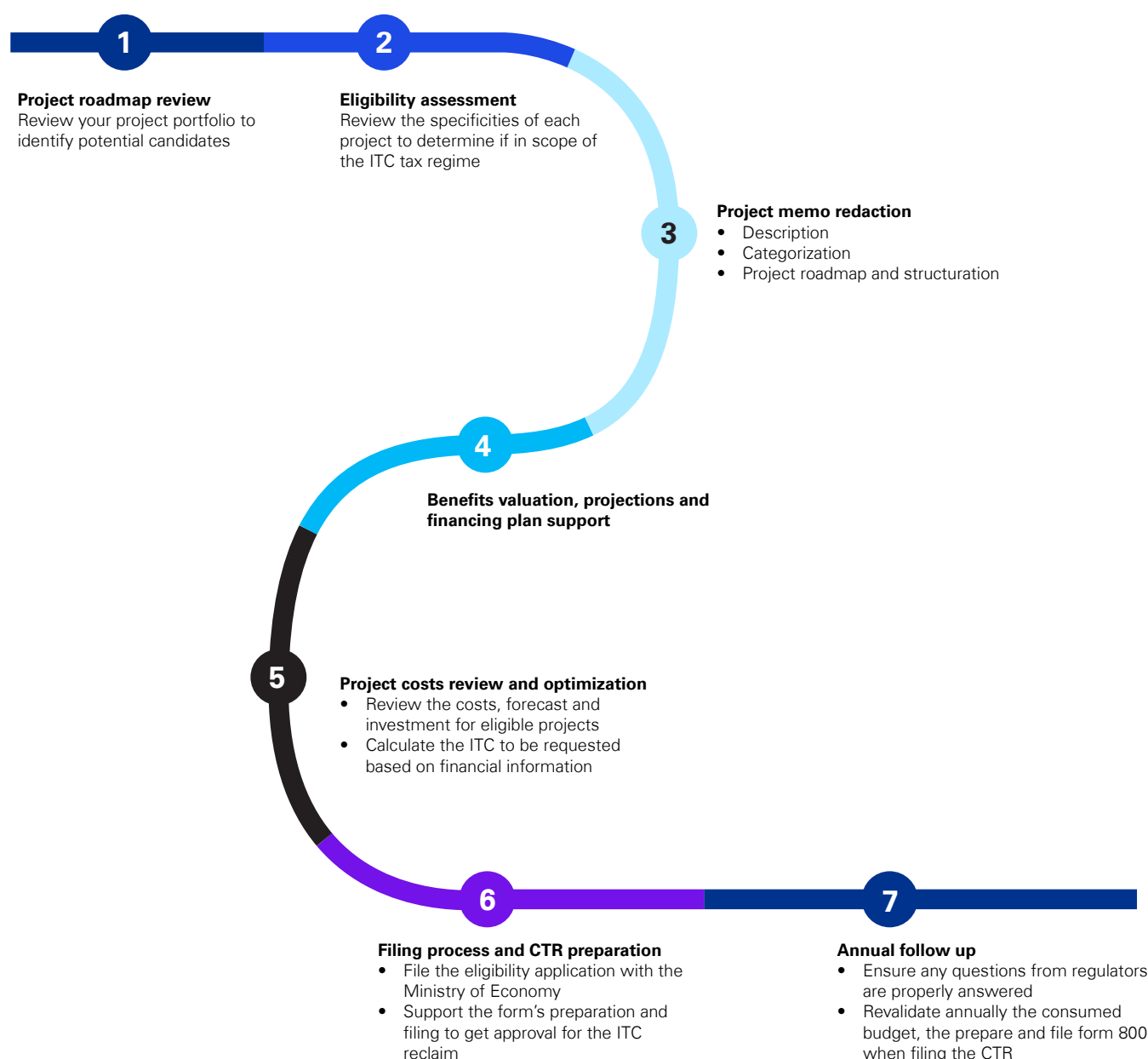
The financial institution includes an annual certificate issued by the Ministry of Economy when filing its corporate tax return (CTR) with form 800.

Companies must request this annual certificate two months after the year-end that the new ITC was claimed, and the Ministry of Economy will issue the certificate within nine months of that year-end.

The certificate will only cover investments and operating expenses made or incurred after the eligibility application was submitted.

KPMG can help you identify whether your new projects can benefit from this 18% tax incentive

Our approach:



Questions that may be raised

1

Have we considered the tax incentive that we could receive if we perform a digital transformation or ecological and energy transition project?

2

Do we have existing digital or ecological and energy transition projects that are starting soon or have recently begun?

3

Do we have a project governance in place that ensures ITC eligibility from inception and that related information is gathered efficiently?

By

Edouard Fort

Partner, Tax - Financial Services

E: edouard.fort@kpmg.lu

Banking data strategies: leveraging data governance, cloud implementation and data fabric architectures

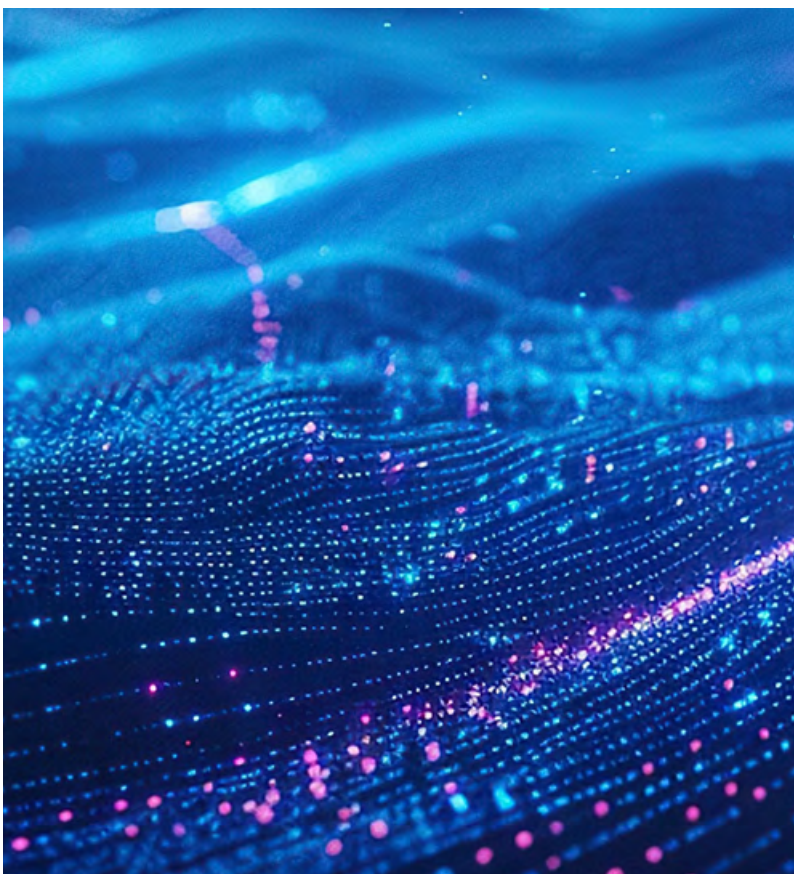
Effective data management not only drives operational efficiency but also enhances customer experience and ensures regulatory compliance.

Critical components for achieving a robust banking data strategy must consider the implementation of solid data governance frameworks, the adoption of cloud technologies for agility and AI readiness, and the pursuit of data fabric architectures to unify data management.

1. The cornerstone: robust data governance and data management frameworks

At the heart of any effective data strategy lies a solid data governance framework. The Data Management Association's Data Management Body of Knowledge (DAMA DMBOK) provides a comprehensive guide for organizations to systematically manage data assets. For banks, adhering to these principles is not just best practice — it's imperative.

- **Regulatory compliance:** banks operate under stringent regulations, including the General Data Protection Regulation (GDPR), Basel III, and Anti-Money Laundering (AML) laws. A robust data governance framework ensures compliance by establishing clear policies and procedures for data handling, avoiding hefty fines and reputational damage as a result.

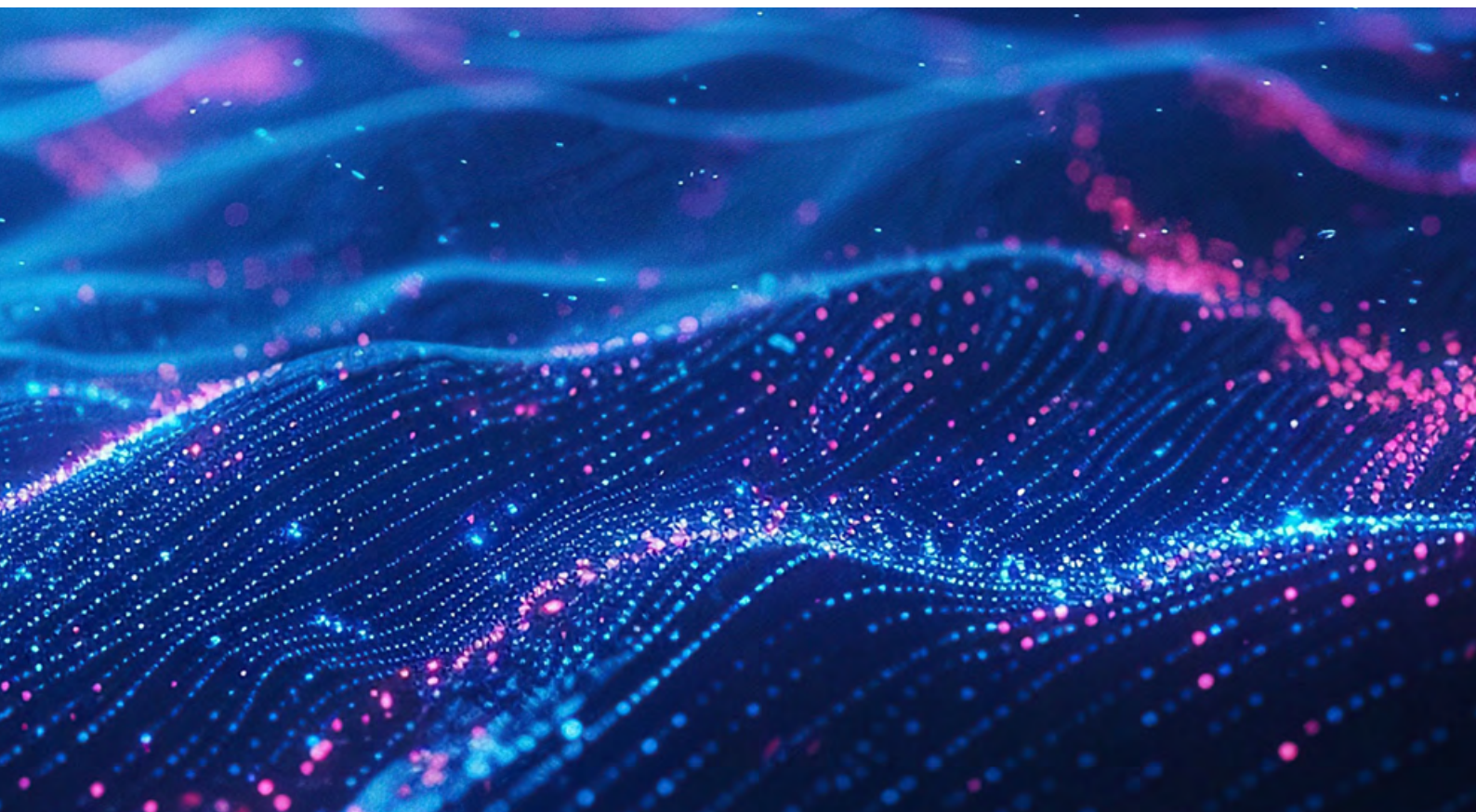


- **Data quality and integrity:** high-quality data is a must for accurate analytics and decision-making. By implementing data entry, validation and maintenance standards, banks can ensure data integrity across all systems.
- **Security and privacy:** with sensitive customer information at stake, data security is paramount. A solid framework enforces access controls, encryption and regular security audits to protect against breaches and cyber threats.
- **Risk management:** effective data governance enhances risk assessment capabilities. By having accurate and timely data, banks can better predict and mitigate financial risks, fraud and other threats.

2. Embracing cloud implementation for modernization and AI readiness

Transitioning data management frameworks to the cloud is a strategic move that offers numerous benefits aligned with modern banking needs.

- **Scalability and flexibility:** cloud platforms provide scalable resources that can adjust to the bank's data volume demands without significant capital investment in hardware. This flexibility is crucial for accommodating growth and fluctuating workloads.
- **Cost efficiency:** by reducing the need for physical infrastructure and maintenance, cloud adoption lowers operational costs. Pay-as-you-go models allow banks to optimize spending based on actual usage.



- **Innovation enablement:** cloud services offer access to cutting-edge tools and technologies, including advanced analytics, machine learning, and AI capabilities. This access accelerates innovation and time-to-market for new services.
- **Agility:** cloud environments support agile development methodologies, enabling faster deployment of applications and services, as well as nimble responses to market changes.

3. Pursuing data fabric architectures as a strategic approach

Data fabric architectures represent the next evolution in data management, offering a unified platform that integrates data across disparate sources and systems.

- **Definition and purpose:** a data fabric is an architectural approach that provides a seamless data management environment. It connects various data repositories, both on-premises and in the cloud, enabling consistent data handling.
- **Enhanced data accessibility:** with data fabric, banks can achieve real-time data access and analytics. This capability supports informed decision-making and personalized customer experiences.
- **Integration with legacy systems:** banks often struggle with outdated legacy systems. Data fabric architectures allow for the integration of these systems with modern applications, ensuring historical data remains accessible and valuable.
- **AI and machine learning integration:** by unifying data sources, data fabric facilitates the deployment of AI and machine learning models across banks, leading to predictive analytics and process automation.

Additional considerations for a comprehensive data strategy

- **Customer-centric focus:** leveraging data effectively allows banks to offer personalized services, improve customer satisfaction and build loyalty. Data-driven insights enable tailored product offerings and proactive customer engagement.
- **Data culture and skills development:** Cultivating a data-driven culture is essential. Investing in employee training ensures staff can leverage new tools and technologies effectively, maximizing the return on data strategy investments.
- **Case studies:** JPMorgan Chase has successfully implemented a data fabric architecture, enhancing its data accessibility and analytics capabilities, leading to improved risk management and customer service.



Potential challenges and mitigation strategies

- **Data security and concerns:** while cloud environments offer robust security measures, they also present new risks. Implementing strong encryption, multi-factor authentication and regular security assessments can mitigate these concerns.
- **Regulatory hurdles:** compliance with data residency and privacy laws can complicate cloud adoption. Banks should work closely with legal teams and regulators to ensure cloud deployments meet all legal requirements.
- **Change management:** transitioning to new data strategies requires careful change management. Clear communication, stakeholder engagement and phased implementation can help ease the transition and promote adoption across the organization.

Conclusion

A modern banking data strategy that combines robust data governance frameworks, cloud implementation and data fabric architectures positions banks for success in a competitive market. By addressing regulatory requirements, enhancing operational efficiency and leveraging advanced analytics and AI, banks can transform data into a powerful asset that drives growth and innovation. Embracing these strategies not only meets the immediate challenges but also sets the foundation for future technological advancements and evolving customer expectations.



Questions that may be raised

1 How well does our current data strategy align with our overall business goals?	6 How often do we encounter data quality issues, and how do they impact our operations?
2 Do we have a well-structured data management framework which supports our risk and IT architectures?	7 How do we ensure data integrity and compliance across different jurisdictions?
3 What should we do with our current, limited Data Warehouses (DWH) and the proliferation of Excel files being created outside of our financial reporting (FINREP) and common reporting (COREP) systems?	8 Are we able to integrate data from various sources and provide consolidated reports across the business lines or external stakeholders?
4 Do we have the right data aggregation capabilities to ensure clean and reliable data from clients, which approximately aligns with regulator expectations?	9 How scalable and flexible is our data architecture to support current and future trends?
5 How effectively do we manage our data across different functions and departments?	10 Do we have a well-governed “single source of truth” data layer that allows effective data identification, analysis of data flows, and reporting?

By

Lana Khoury

Partner, Technology Advisory

E: lane.khoury@kpmg.lu

Artificial intelligence and governance in banking

The use of artificial intelligence (AI) has become an integral part of the financial sector, particularly in banking, ranging from customer service chatbots to complex financial modeling and risk management tools. While the opportunities are immense, the risks are equally significant, making AI governance a critical area for compliance, risk management and ethical operation. Effective AI governance ensures that AI systems are developed and used responsibly, complying with regulatory requirements like the forthcoming EU AI Act.

Understanding AI governance in banking

AI governance in the banking industry involves the structured management and oversight of AI systems to ensure they are developed and deployed in a responsible, transparent and ethical manner. This includes setting principles, policies and frameworks to address AI-related risks, such as biases in algorithms, data privacy issues and potential misuse of AI technology. AI governance should focus on enhancing transparency, fostering accountability and ensuring that AI-driven initiatives are aligned with both business goals and regulatory standards.

Key objectives of AI governance in banking

- 1. Risk management and compliance:** AI governance helps banks manage risks associated with AI, including operational, reputational and compliance risks. By establishing clear guidelines and monitoring frameworks, banks can proactively identify and mitigate potential harms arising from the use of AI.
- 2. Trust and transparency:** effective AI governance ensures AI systems are transparent in their decision-making processes, which is essential for maintaining consumer trust and confidence.
- 3. Ethical AI deployment:** ensuring AI systems adhere to ethical guidelines is fundamental. This involves implementing policies that prevent discriminatory practices and promote fairness, especially when AI is used for sensitive areas like loan approvals, credit scoring, or customer profiling.
- 4. Alignment with regulatory requirements:** the EU AI Act mandates that AI systems, especially high-risk systems like those used in banking, comply with stringent requirements. AI governance frameworks help banks ensure their AI systems meet these legal standards.

Components of an effective AI governance framework

An effective AI governance framework in the banking sector should include several layers:

- 1. Organizational strategy:** reimagining existing governance models to incorporate AI-specific risks and define an operating model that fits the bank's unique structure. It should consider risk management, regulatory requirements and strategic alignment.
- 2. Defining AI principles:** establishing clear principles for AI development and deployment, such as transparency, accountability and fairness, which guide the organization in building and maintaining a robust AI governance framework.
- 3. Policies and standards:** creating comprehensive policies, standards and procedures that align AI operations with internal and external regulatory requirements like the EU AI Act.
- 4. Design, implementation, and control:** implementing the policies across various business lines and ensuring AI technologies are used responsibly, effectively and in compliance with set standards.
- 5. Metrics, monitoring, and reporting:** developing metrics to assess AI system performance and ensure ongoing compliance with AI governance policies.

Challenges implementing AI governance in banking

Despite its necessity, implementing AI governance in the banking sector is not without challenges. Banks often struggle to balance innovation and compliance, particularly when integrating AI governance frameworks with existing risk management and compliance models.

Common challenges include:

- 1. Complexity of AI systems:** AI systems, especially those using machine learning, can be complex and opaque, making it difficult to explain their decision-making processes.
- 2. Data privacy concerns:** banks handle vast amounts of sensitive data. Therefore, ensuring AI systems comply with data privacy regulations, such as GDPR, adds an additional layer of complexity.
- 3. Regulatory uncertainty:** the evolving nature of the AI regulations, like the EU AI Act, means banks must continuously adapt their governance frameworks to stay compliant.
- 4. Cultural and organizational barriers:** implementing AI governance requires buy-in from all levels of the organization. Resistance to change or a lack of understanding of AI risks can impede the effective implementation of governance frameworks.

The EU AI Act

The EU AI Act is a landmark piece of legislation aimed at regulating the use of AI in the EU. It classifies AI systems into different risk categories, ranging from minimal to high-risk, and establishes compliance requirements based on these classifications. The legislation, which entered into effect in August 2024, will apply in a staggered timeline from February 2025 until August 2026, where all rules of the AI Act become applicable, including obligations for high-risk systems.

High-risk systems, which include many applications in the banking sector, must comply with stringent requirements, including:

1. **Risk management:** conducting regular risk assessments and implementing risk mitigation measures for AI systems.
2. **Transparency requirements:** ensuring AI systems provide clear information on their functioning and limitations.
3. **Data governance:** establishing robust data governance practices to ensure data quality and mitigate biases.
4. **Human oversight:** implementing human oversight mechanisms to prevent or minimize potential risks associated with AI systems.

The EU AI Act has several implications for AI governance in the banking sector, including:

1. **Alignment of AI systems with EU requirements:** banks must ensure their AI systems meet the AI Act's requirements, especially high-risk systems like those used for credit scoring or fraud detection. This involves implementing comprehensive risk management, transparency, and data governance measures.
2. **Enhanced accountability:** the EU AI Act places a strong emphasis on accountability, requiring banks to maintain detailed documentation of their AI systems, including records of risk assessments, data management practices and compliance efforts.
3. **Strengthened oversight and control:** banks must establish robust oversight mechanisms to ensure that AI systems operate as intended and do not pose undue risks to customers or the financial system.
4. **Focus on ethical AI:** the EU AI Act encourages the use of AI systems in a manner that respects fundamental rights, including non-discrimination, fairness and transparency. Banks must ensure their AI governance frameworks address these ethical considerations.

Conclusion

AI governance in banking is critical for ensuring the responsible, transparent, and compliant use of AI technologies. As the EU AI Act comes into effect, banks must align their AI governance frameworks with the new regulatory requirements to manage risks effectively and maintain customer trust. By doing so, they can harness the full potential of AI while safeguarding against the risks associated with its use.

This integration of AI governance and regulatory compliance not only helps banks avoid legal penalties but also promotes the ethical and trustworthy use of AI, which is essential for long-term success in the digital age. As AI technologies continue to evolve, banks will need to continuously adapt their governance frameworks to stay ahead of regulatory developments and maintain their competitive edge.

Questions that may be raised

1

Do we have a plan in place to build competencies and emerging skillsets critical to understand the risks of using AI across the bank?

5

How will we govern and monitor compliance with regulatory bodies to address AI-related risks and ethical considerations?

2

Are we prioritizing cultural changes to unlock the potential of AI and a better future of work?

6

Do we understand the difference between white and black box models and their impact on risks?

3

Have we thoroughly examined how to improve our processes before applying AI?

7

Are we addressing the importance of data and data management in the context of AI?

4

What risks have we identified, and have we categorized and prioritized them accordingly?

8

Do we understand the four levels of the EU AI Act and whether our organization will classify as a provider, deployer or both?

By

Lana Khoury

Partner, Technology Advisory

E: lane.khoury@kpmg.lu

EMIR Refit

Twelve years after the European Market Infrastructure Regulation (EMIR) was adopted, derivative trading is still undergoing significant regulatory changes. On 29 April 2024, the EMIR Refit entered into force, a large-scale update to enhance the reporting quality of over-the-counter derivatives (OTCs) and exchange-traded derivatives (ETDs).

EU financial institutions engaging in derivative trading must report every transaction execution, modification, early termination and valuation (including collateral) to an authorized trade repository no later than the next business day.

While the market is still digesting the EMIR Refit's new rules, even more changes are on the horizon thanks to next year's "EMIR 3.0" update.

The four pillars of EMIR Refit

1. Reporting under new validation rules

- EMIR Refit adopts a new end-to-end, XML-based reporting common to all trade repositories, containing new fields, format changes and modifications to the reported values.
- The 89 new reporting data fields bring the total number of reportable fields to 203.

2. Mandatory delegation reporting

- When a financial counterparty (FC) deals with a non-financial counterparty (NFC), the FC is responsible and legally liable for reporting on the NFC's behalf.

3. Regulator notification of significant reporting issues

The financial institution must proactively notify the regulator of any:

- Significant misreporting and reporting errors
- Any obstacles that may prevent reporting within the deadline.

4. New trade repository controls and feedback messages

- Trade repositories must check the reports they receive and reconcile any outstanding ones.
- They must provide feedback reports concerning rejections, reconciliations and data quality.

Data quality monitoring

This adaptation of reporting rules is accompanied by increased regulator supervision, making data quality monitoring essential. The CSSF's new targeted, results-based data quality approach is based on 19 data quality indicators and an unlimited number of annual data quality exercises. Each entity's EMIR reporting quality will be a sign of its overall regulatory health.

Therefore, credit institutions must adequately oversee the accuracy, completeness and timeliness of this reporting. This can range from sample testing to implementing control tools depending on the entity's resources, capabilities and risk appetite.

Current challenges

- Banks are struggling to streamline their regulatory data management processes that remain siloed and manually intensive across multiple people-dependent reporting layers. In addition, each respective entity of a global bank may have different processes in place. Therefore, scaling processes and controls is an opportunity to reduce costs and risks.
- Correct counterparty classification and data availability are significant challenges for reporting under EMIR Refit rules.
- The EMIR Refit's concepts of the "entity responsible for reporting" and the "reporting counterparty" can cause confusion when providing third-party reports or when delegating reporting.
- It's essential that banks adequately understand feedback messages from trade repositories to improve their data quality.
- CSSF notifications for misreporting or reporting errors are subject to the significance calculation and require banks to fully understand the new validation rules.
- EMIR Refit comes with a renewed involvement of internal control functions in EMIR-related processes through compliance reviews and internal audits; external findings from supervisory authorities can lead to fines.

EMIR 3.0

Concerned banks and financial institutions must also keep EMIR 3.0 in mind, which is expected to go live in mid-2025. Its major changes relate to certain entities' obligation to have active accounts at EU central clearing counterparties, alongside focus on EMIR data quality controls.

Questions that may be raised

1

Have we established and adapted an EMIR framework that is tailored to the EMIR Refit and uplifted CSSF expectations?

3

Have any initial obstacles to implementing the EMIR Refit required us to notify the CSSF?

2

How do we control the accuracy, timeliness and completeness of EMIR Refit reporting?

4

Are our internal control functions sufficiently involved in EMIR processes, and are errors adequately escalated to authorized management?

By

Thor-Hagen Scheller

Director, Advisory

E: thor-hagen.scheller@kpmg.lu

kpmg.lu

home.kpmg/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

©2024 KPMG S.à r.l., a Luxembourg entity and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International.