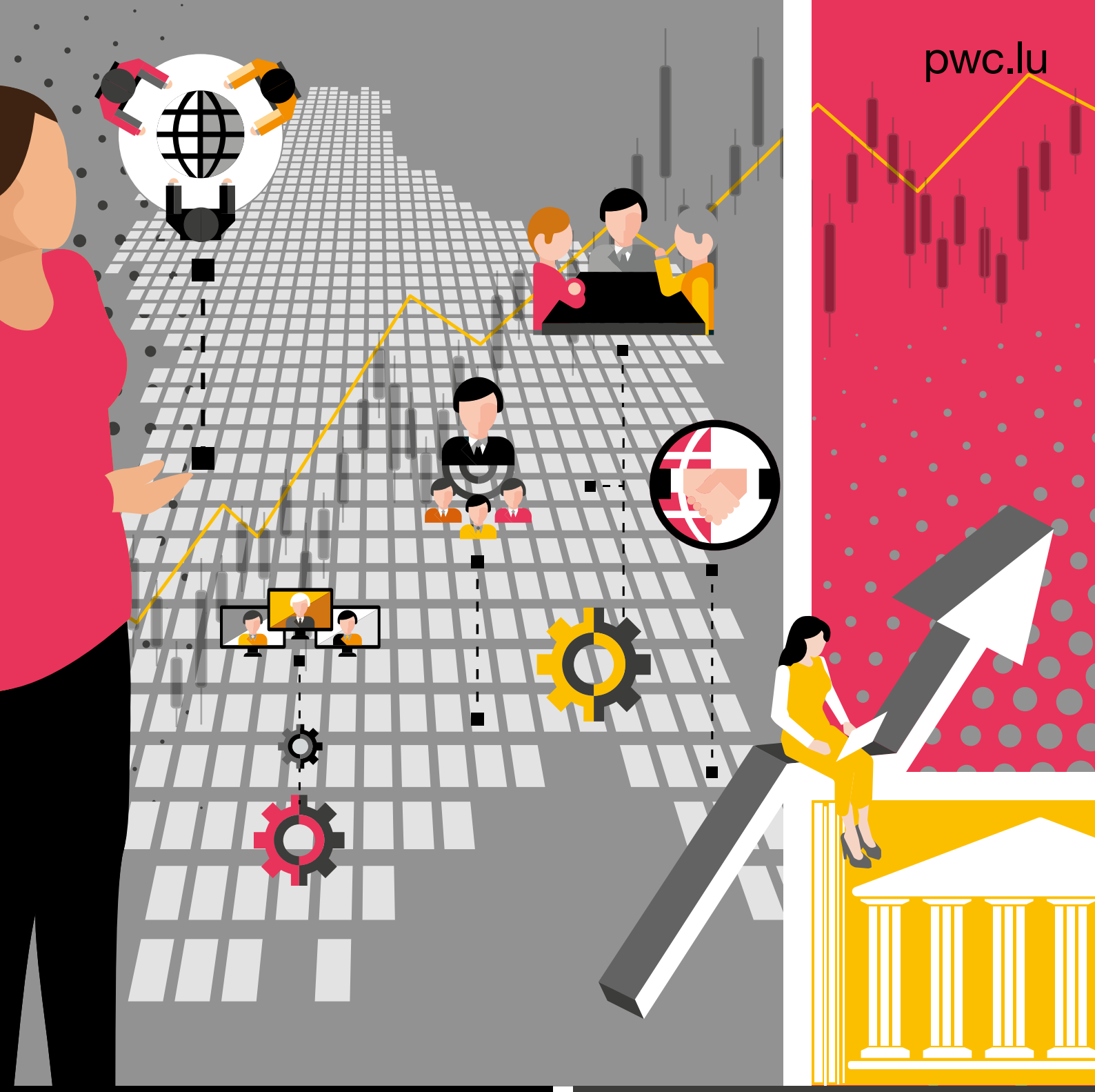


Banking in Luxembourg

Together towards another decade of resilience

Executive Summary

pwc

Introduction

Having withstood the geopolitical and macroeconomic turbulence of recent years alongside the banking crisis of early 2023 with relative ease, the European Union's banking sector is on strong footing. To a large degree, this resilience is a byproduct of the formal establishment of the EU banking union ten years ago.

As per the Single Supervisory Mechanism (SSM), the European Central Bank has been endowed with supervisory powers since 2014, directly overseeing the EU's largest banks. It also indirectly oversees smaller banks through national competent authorities. In December 2023, it published its latest SSM Supervisory Priorities for 2024-2026.

Renowned for its time-honoured stability and prudence, Luxembourg's banking sector has actively implemented the ECB's SSM Supervisory Priorities.

Our report seeks to provide the leadership of the Luxembourgish banking sector with practical recommendations regarding the supervisory priorities, alongside two areas not formally under the ECB's purview.

Resilience to immediate macro-financial and geopolitical shocks

Concerning credit risk and counterparty credit risk management frameworks, there are a host of actions that the leadership Luxembourgish banking sector should consider.

The Chief Risk Officer (CRO) and the Credit Committee need to develop a deep understanding of the European Banking Authority's guidelines on loan origination and monitoring (LOM) and analyse the LOM data in an aggregate manner to ensure that the bank abides by the guidelines. The CRO should also take the lead in conducting the bank's stress tests and reverse stress tests with the support from the Chief Financial Officer (CFO) who would provide much of the data needed. Should the position exist, the CRO should consult with the Chief Sustainability Officer (CSO) for feedback and advice on the overall environmental, social and governance (ESG) risks that the bank may encounter and incorporate them in the tests. The CFO should separately ensure that the bank abides by IFRS 9.

The CRO will need to envisage situations that would prompt institutional and high-net worth clients to rapidly withdraw their deposits, and use these scenarios to test the reliability of the bank's asset and liability management frameworks. The Chief Executive Officer (CEO) should then take the lead in devising new strategies for the bank's liquidity and funding, with the goal of achieving diversified funding structures that help manage risks stemming from interest rate changes or changes in customer behaviour. The CEO should also understand how the bank is exposed to the Interest Rate Risk in the Banking Book (IRRBB) and ensure that the IRRBB framework is reviewed and evaluated on a regular basis.

Managing Governance and ESG Risks

The chairperson of the bank's board of directors and the CEO should promote a culture of openness and constructive dialogue across the organisation, and should demonstrate openness, humbleness, humility and a genuine desire to be in contact with the bank's staff while avoiding a domineering attitude that fails to acknowledge different points of view. The senior management should feel empowered to constructively challenge the board and offer alternative recommendations when necessary – with the inverse also being true.

The boards of directors in Luxembourg's banks should establish succession and onboarding plans to ensure new members are provided with all the information and knowledge necessary (i.e. the bank's history; its risk exposure; areas in which their expertise comes into play etc.) from their older, more-experienced peers. Boards should also adopt a holistic approach to diversity (gender, age, professional, ethnic and geographic backgrounds) and strive to increase diversity while being careful to avoid increasing diversity just for diversity's sake or to fill in a certain quota.

A policy should be established within the bank to define which compliance documents should reach the board in their entirety and which ones should be provided in a summary format, as this will allow the board to spend more time on strategic matters. In addition, the board should work closely with the Chief Operating Officer (COO), the Chief Compliance Officer (CCO), the CRO and the internal audit function to develop an understanding of the multifaceted risks the bank faces, the expected future regulatory developments, and how to cope with them and even unlock opportunities.

Banks should also address deficiencies in risk data aggregation and risk reporting (RDARR). This can be done either through collaborative efforts by the CRO, the Chief Information Officer (CIO) and the CFO, or by giving responsibility for all RDARR-related matters to a data office or a Chief Data Officer. Banks should demonstrate how they are putting efforts into closing the RDARR gaps and deficiencies by delineating responsibilities at a granular level, whereby each data owner inputs the data to be used for KPIs, stress tests and reverse stress tests. Ultimately, RDARR would greatly benefit the board of directors as the data can be used to inform the bank's strategy.

As for the ESG-related risks that Luxembourg's banks are faced with, CROs and CCOs need to determine them while the former should develop and enforce climate-related risk policies. The CEO, on the other hand, should guide efforts towards establishing or refining the bank's net-zero transition plan and ensure that it reflects market risk and operational risk assessments. This plan would be overseen by the CSO, who would ensure that the bank's green asset ratio is gradually increasing and collaborate with the CRO and CCO to identify ESG-related opportunities.

Progress in the digital transformation and digital operational resilience

For a bank's digital transformation to be successful, the alignment of the members of the C-Suite over a clear and transparent governance structure and oversight processes is a must. The CEO should set the general objectives of the digital transformation strategy and ensure that they align with the bank's strategic objectives and its risk appetite, while the COO should ensure that back offices are adequately prepared.

The CIO should coordinate and receive feedback and guidance from other members of the C-Suite on how the digital transformation can and should affect their respective responsibilities and operations. The CFO, on the other hand, should proactively identify any financial risks that might arise from the digital transformation and communicate them to the rest of the C-Suite, while the CRO would need to integrate how the digital strategy aligns with the bank's risk appetite.

Luxembourg's thriving fintech ecosystem has already played a role in pushing banks to adopt Cloud and Generative Artificial Intelligence (GenAI) solutions, and they will need to continue investing in their digital transformation. In partnership with the CRO and the Chief Information Security Officer (CISO), the CIO needs to ensure that the bank's overarching digital transformation is subject to rigorous risk assessments that cover all potential cyber-related risks that may arise. Risk management should be fully embedded in the design and implementation of the digital transformation strategy, with adequate mechanisms for cyber-related risk monitoring and reporting.

As for banks' digital operational resilience, the implementation journey of the EU's Digital Operational Resilience Act (DORA) is a multi-faceted process that requires the input and collaboration of all members of the C-Suite, including the CISO. Within the bank, the latter plays a strategy role (i.e. defining the bank's cybersecurity objectives and goals), a coordination and oversight role (i.e. ensuring the bank has processes and mechanisms to withstand and recover from a cyberattack), and a control and reporting role (i.e. verifying the effectiveness of the bank's cybersecurity measures).

When it comes to the bank's emergency response and disaster recovery plan, the CIO is responsible for making sure that the ICT assets needed to embark on the recovery plan are in place, the COO and the communications department need to ensure that the cyber attack is communicated in an adequate manner to all internal and external stakeholders, and the CEO must oversee the whole recovery process, ensuring that each part is properly implemented.

The CRO and the CCO should take the lead in the oversight of ICT third-party providers, ensuring that the outsourcing chain is transparent. The CIO should determine which providers can ensure long-term resilience and whether the current setup can guarantee the bank's digital operational resilience. Regarding the register of information on ICT third-party service providers prescribed by DORA, the bank's CRO or the CCO will need to maintain it and ensure it is up-to-date and that it is part of the bank's broader outsourcing register which contains non-ICT outsourced services.

Tax Resilience and Innovation

The CEO and the CFO should consider establishing a department dedicated to managing tax affairs and weigh such a consideration against prospective outsourcing arrangements which provide a cost-effective solution that unlocks a wide array of tax-related benefits and highlights the different tax-related risks the bank faces.

Responsibility for the implementation of the EU's Central Electronic System of Payment Information (CESOP) will have to be spread between several actors within the bank. For the banks that do have a Head of Tax Affairs, the latter will need to cooperate and coordinate closely with the COO, CFO and the CIO to ensure that the adequate ICT processes and reporting mechanisms are in place. As for banks where there is no Head of Tax Affairs, the responsibility will fall on the COO, the CFO and the CIO.

The CEO take the lead in directing efforts towards understanding how the recently-announced digital and ecological transformation (DET) tax credit can benefit the bank. With regards to the bank's digital transformation, the tax function is likely going to be significantly affected by artificial intelligence. In banks that have a department for managing tax affairs, the department's head and the CIO should examine all the potential opportunities and efficiency gains that GenAI solutions and services can bring.

Banks with a strong ESG track record should consider publishing a tax transparency report on an annual basis. The Global Reporting Initiative's standard for public reporting on tax, GRI 207, can be used as the report's foundation.

Coping with Heightened Financial Crime Risks

The CCOs and CROs of Luxembourg's banking sector will need to keep a keen eye on the European Commission's Anti-Money Laundering (AML) package and understand how the new AML Regulation will affect them and what the role of the new AML Authority will be. They will need to ensure that the bank's AML policies, procedures and controls are all up-to-date and aligned with applicable regulations.

Given that many banks struggle to attract, retain and upskill staff with AML experience, the COO should closely cooperate with the CCO and/or CRO to understand what the bank's AML-related operational deficiencies are and how they can be resolved. As for GenAI applications in AML operations, such solutions need to be seen as a complement rather than a replacement for human expertise. The CCO, the CRO and the CIO should cooperate closely to determine what processes should be prioritised, what solutions should be enacted, and what actions should be taken (e.g. upskilling staff). The CRO needs to ensure that robust governance frameworks are in place to oversee and monitor the development, testing and deployment of AI solutions.

The CEOs of Luxembourg's banking sector should regularly consult with the CCO, the CRO, the COO and, increasingly, the CIO, regarding the bank's AML processes and procedures. They should not shy away from taking the necessary actions to remediate any shortcomings that may be identified. As for the board of directors, the tone at the top is crucial, and the chairperson and the directors need to promote a strong culture of AML compliance.

Contacts

Julie Batsch
Partner, Banking & Capital Markets Leader
+352 49 48 48 2467
julie.batsch@pwc.lu

Jörg Ackermann
Partner, Advisory Banking
+352 49 48 48 4131
jorg.ackermann@pwc.lu

Björn Ebert
Partner, Financial Services Leader
+352 49 48 48 2256
bjorn.ebert@pwc.lu

Cécile Liégeois
Partner, Clients & Markets Leader
+352 49 48 48 2245
cecile.liegeois@pwc.lu

Michael Weis
Partner, Forensics & Anti-Financial Crime Leader
+352 49 48 48 4153
michael.weis@pwc.lu

Cécile Moser
Partner, Assurance
+352 49 48 48 5617
cecile.moser@pwc.lu

Murielle Filipucci
Partner, Global Banking & Capital Markets Tax Leader
+352 49 48 48 3118
murielle.filipucci@pwc.lu

Patrice Witz
Partner, Digital Leader
+352 49 48 48 3533
patrice.witz@pwc.lu

Nenad Ilic
Partner, Banking & Capital Markets Tax Leader
+352 49 48 48 2470
nenad.ilic@pwc.lu

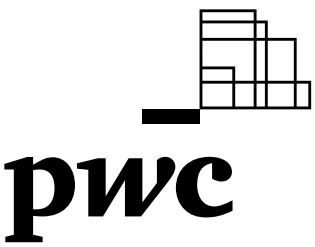
Ryan Davis
Partner, Regulatory & Compliance
+352 49 48 48 3580
ryan.c.davis@pwc.lu

Jean-Philippe Maes
Partner, Regulatory & Compliance
+352 49 48 48 2874
jean-philippe.maes@pwc.lu

Isabelle Melcion-Richard
Managing Director, Regulatory & Compliance
+352 49 48 48 2469
isabelle.melcion-richard@pwc.lu

Maxime Pallez
Director, Cybersecurity Governance, Risk & Compliance Leader
+352 49 48 48 4166
maxime.pallez@pwc.lu

www.pwc.lu/banking



PwC Luxembourg (www.pwc.lu) is the largest professional services firm in Luxembourg with over 3,700 people employed from 94 different countries. PwC Luxembourg provides audit, tax and advisory services including management consulting, transaction, financing and regulatory advice. The firm provides advice to a wide variety of clients from local and middle market entrepreneurs to large multinational companies operating from Luxembourg and the Greater Region. The firm helps its clients create the value they are looking for by contributing to the smooth operation of the capital markets and providing advice through an industry-focused approach.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with over 364,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com and www.pwc.lu.