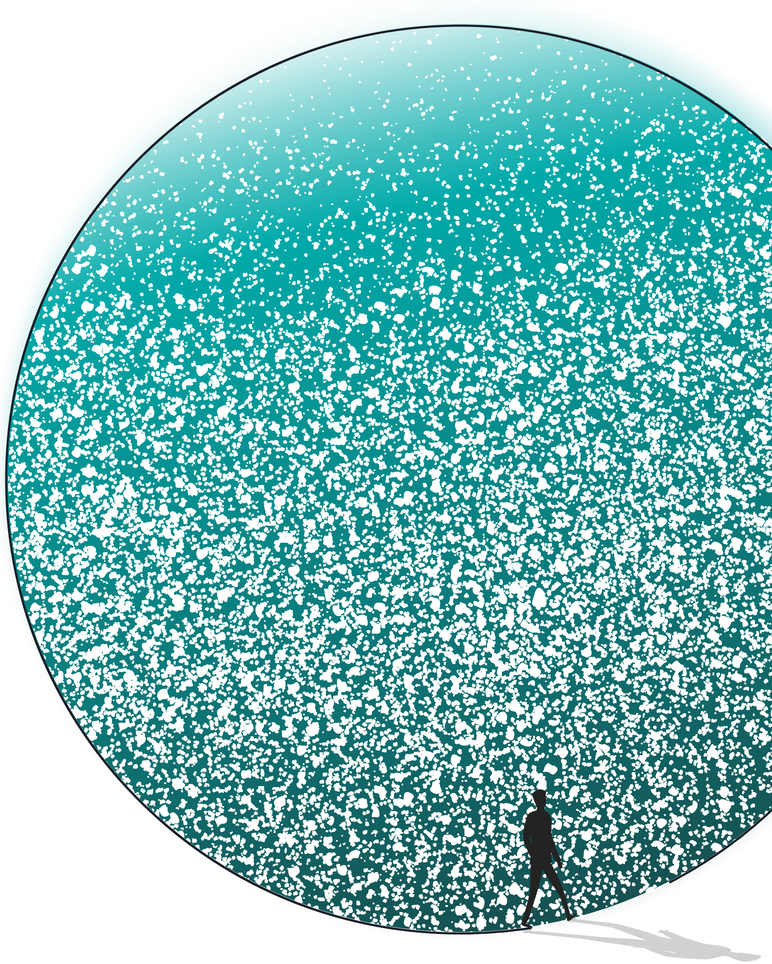
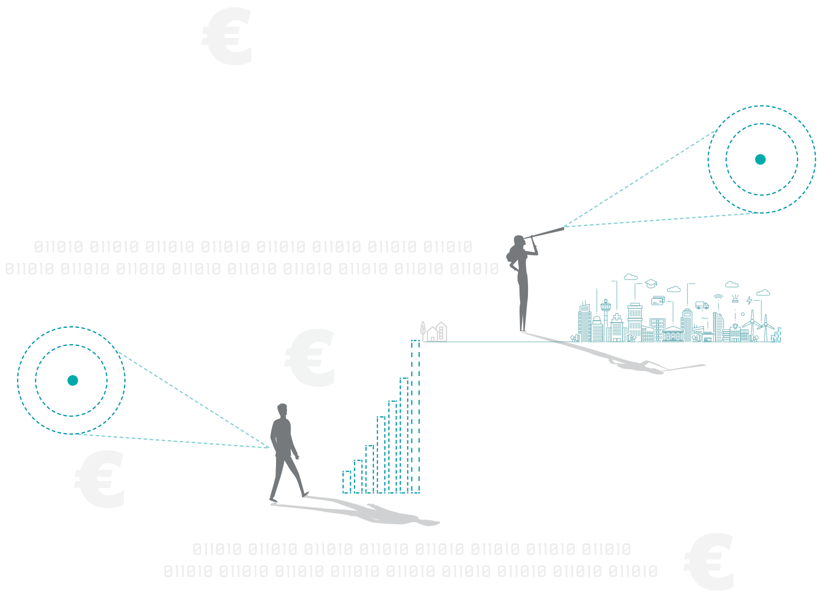


Irish Banking Outlook 2024

Contents



Introduction

As we enter 2024, we delve into the key trends and developments shaping the future of the Irish banking industry.

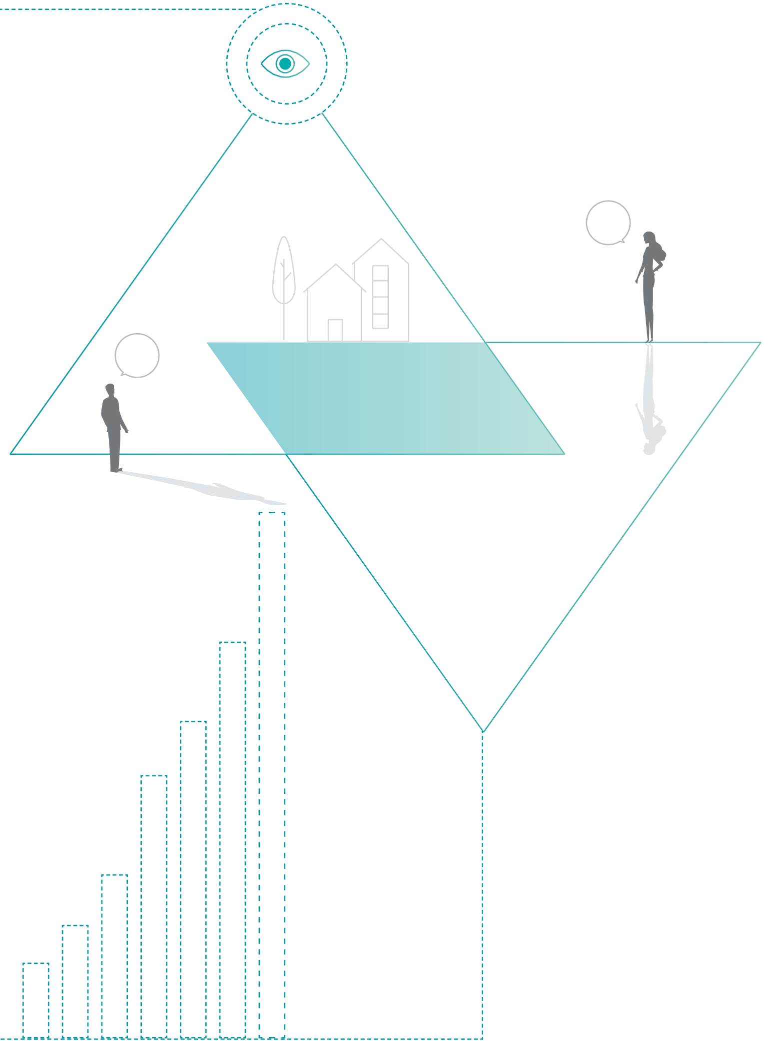
We explore the impact of digital transformation, generative AI, sustainability, data and changing customer expectations on the industry landscape. By understanding these dynamics, stakeholders can better navigate the challenges and seize the opportunities that lie ahead, thereby ensuring the continued vibrancy and resilience of the banking sector which is a cornerstone of Ireland's economy.

Macroeconomic factors

The Irish economy has proven to be highly resilient in the face of a series of disruptive events. However, the balance of risks facing both the Irish and global economies remain tilted to the downside. At present in Ireland, the domestic economy remains strong, but exports are being impacted by the reduction in global demand, with a 6% year-on-year (YoY) contraction in value terms in the first three quarters of 2023.

Insolvencies increased by 26% YoY in the first three quarters of 2023, albeit from a low base. Total numbers remain quite low. In the mortgage market, the number of principal dwelling house mortgages in arrears over 90 days decreased by 8.2% in the year to the end of June 2023. This number will be closely watched as close to 19% of mortgage holders will roll off current fixed term rates over the coming year. The latest available data reveals that average interest rates for new mortgage agreements stood at 4.3% in September 2023, versus a rate of 2.78% in March 2022, pre-interest rate hikes.

Commercial property remains challenged as “price discovery” continues. The rising cost of debt combined with economic uncertainty has led to valuation adjustments, with further yield expansion anticipated for 2024. To date, the rate of NPLs on Irish loan books has been stable, but it remains an area of focus. In Germany, the commercial real estate NPL ratio has increased from 2.1% to 2.9%, with the Central Bank of Ireland recently stating its intention to monitor this data closely. This risk has resulted in tightened credit availability, as pillar banks seek to protect loan books.



Sustainability

EU-listed companies will fall into scope for the Corporate Sustainability Reporting Directive (CSRD) from 1st of January 2024 (reporting in 2025). For many Irish banks, mobilisation of the CSRD project is a challenge given the scale of the requirements. However, there is also an opportunity for the pillar banks to consider their overall sustainability strategy.

In addition, Irish banks will have to meet a substantial new reporting requirement in 2024, by disclosing their Green Asset Ratio (GAR) for the financial year 2023, i.e. their percentage of financed assets which can be classified as sustainable.

From a risk perspective, banks must embed climate risk into risk management, mapping it onto traditional prudential risk categories. Capital treatment and scenario analysis will continue to be focus areas.

Transition planning will be a key area of focus for regulators and will have an impact on how banks steer their business. Regulations and global commitments (e.g. GFANZ) are leading to formalised approaches to transition planning.

Green labels for products are an area of focus for European regulators and the Central Bank. Banks also need to consider latent greenwashing risk within their business. This factor will be brought further into focus by the Central Bank of Ireland's introduction of a revised Consumer Protection Code in 2024, with Climate Matters highlighted as a central theme in the revised code's development. There is currently a public consultation relating to the CPC in progress, but Irish banks can expect to face further climate-related requirements which must be adhered to when engaging with their client base.

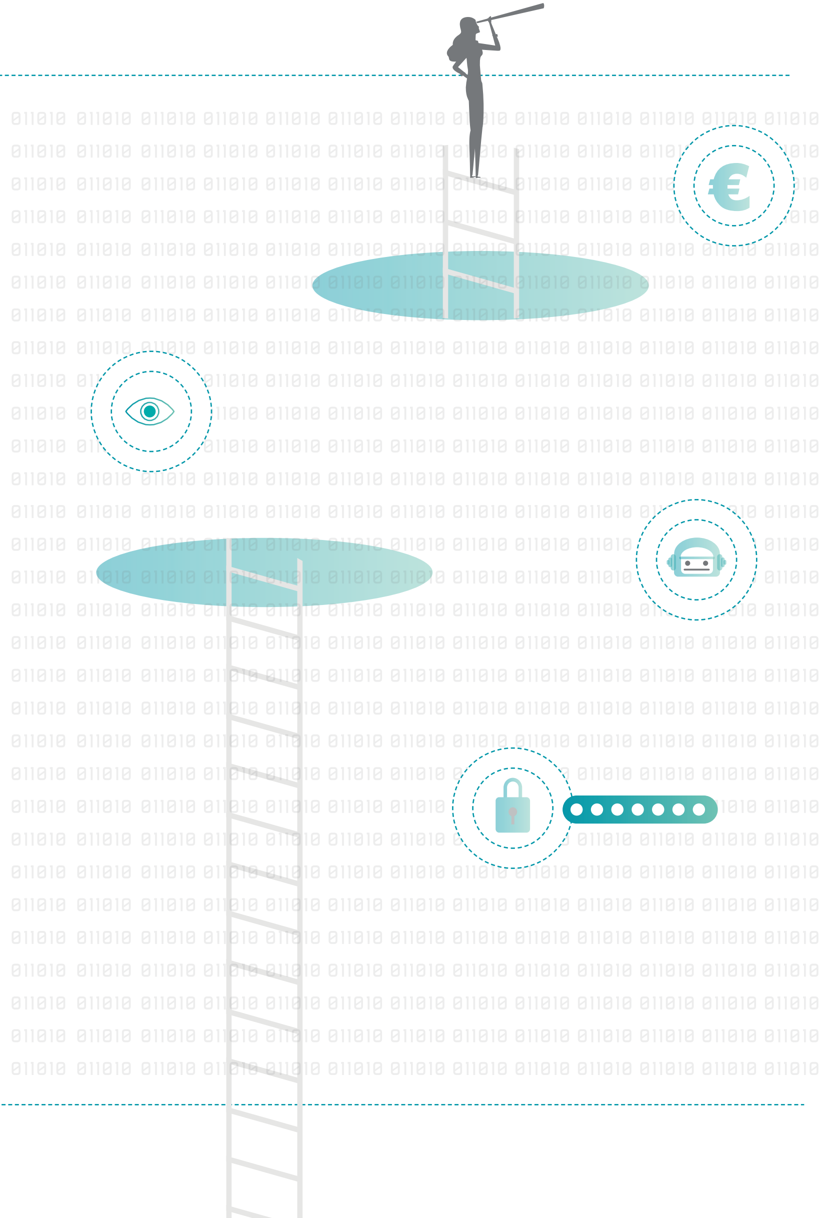
Irish pillar banks will have challenges relating to Environmental, Social and Governance (ESG) reporting in 2024 as they attempt to grasp the sheer volume of data required to meet reporting requirements and to label products adequately. ESG considerations have become integral to the sector, and Irish banks like their European counterparts are developing data frameworks to promote the integration of ESG metrics into their lending and investment decisions.

Data

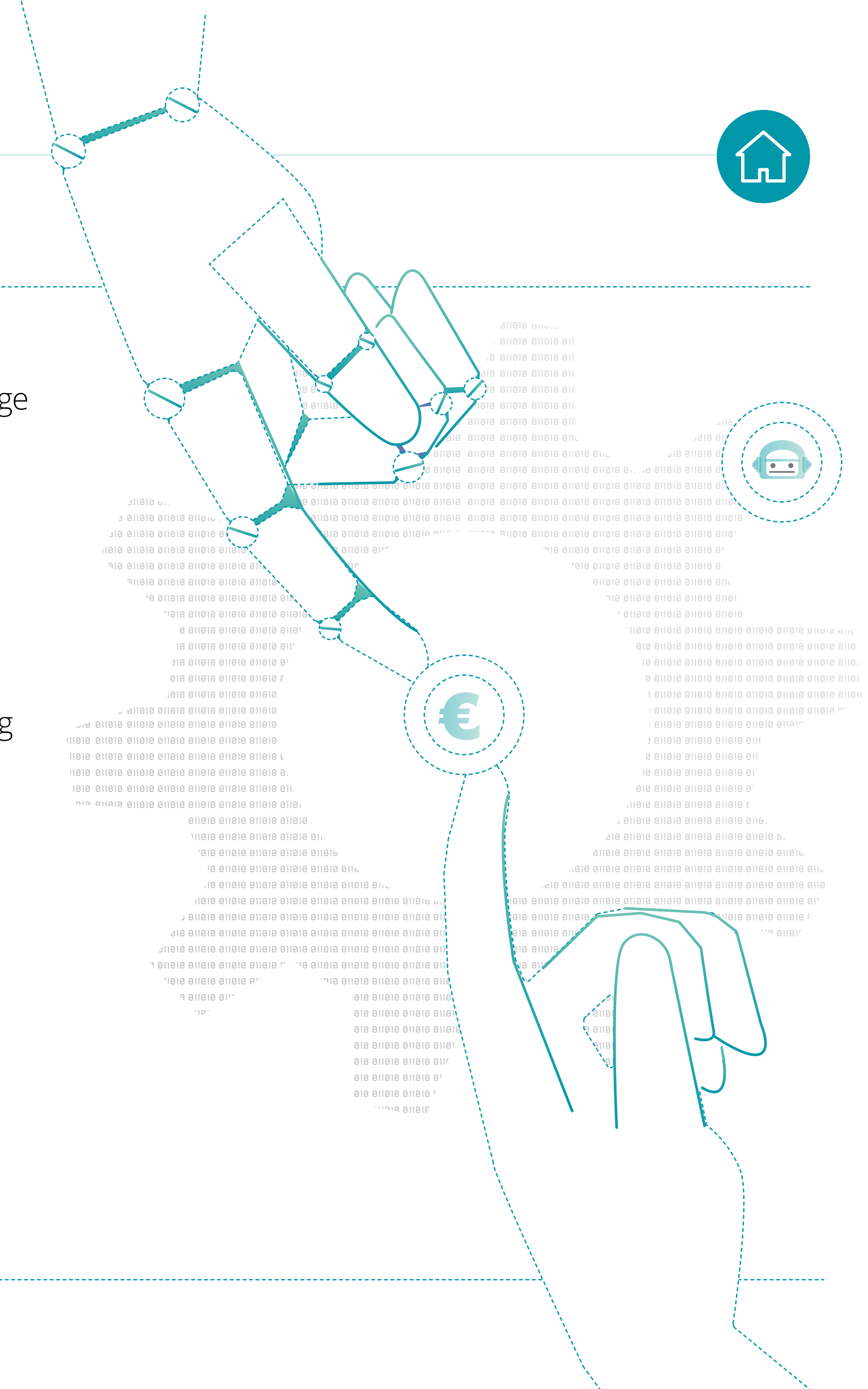
Data management and technology have become increasingly important to the Irish banking system, a theme that looks set to continue into 2024. The implementation of the Basel Committee on Banking Supervision (Principles for Effective Risk Data Aggregation and Risk Reporting (BCBS 239) underscores a growing regulatory emphasis on robust data practices. These regulations necessitate strong data infrastructures which ensure accuracy, transparency, and privacy in all aspects of data handling.

Irish banks are beginning to adopt AI to improve service delivery, leveraging it in areas like customer service through chatbots and in risk assessment for credit scoring. These advancements are helping to improve customer experience and achieve efficiencies. Good data quality and availability are essential for the successful deployment of this technology.

The advent of open banking, propelled by the EU's revised Payment Services Directive (PSD2), is also featuring in banks' data strategies. The facilitating of enhanced data sharing between banks and third-party providers is a significant step towards more customer-centric offerings, while also allowing banks to improve their modelling capabilities in risk and fraud detection.



GenAI



2022 was a watershed year for AI, with the release of consumer-facing applications like Chat GPT, Dall-E and Midjourney capturing the public imagination. While this is leading organisations to re-imagine their products, talent, and business models, attitudes towards the technology vary from enthusiasm for its possible applications to hesitancy and uncertainty around potential consequences.

Much of the uncertainty is a result of stories of misuse or mishandling of sensitive personal data, along with concerns around ethics, implicit bias, and the traceability and trustworthiness of the outputs. These are legitimate concerns that must be addressed.

While regulated markets like banking typically taking a slower and more cautious approach to adopting new technologies, it is still imperative for banks to assess the potential of this technology sooner rather than later.

It is evident that organisations that leverage AI and generative AI technologies will gain a competitive edge by automating repetitive and labour-intensive tasks and unlocking new opportunities for growth and optimisation.

In banking, the competitive disruption can be amplified as agile fintech companies will be able to adapt and leverage these capabilities thereby putting institutional players under increasing pressure.

Starting the AI journey means finding the right use case which will drive value and explore how it can be tested, proven, and deployed effectively in an appropriately governed framework.

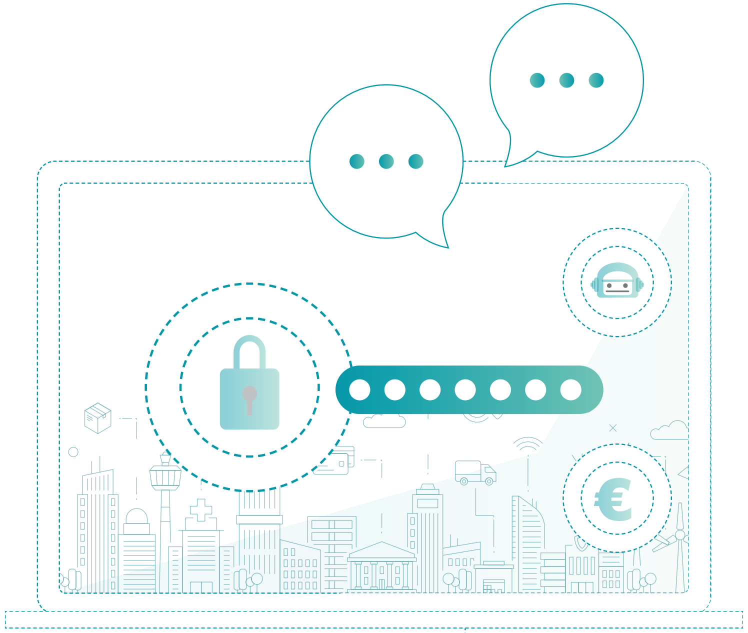
Cybersecurity

Developing the capability to recover from a cyber breach in an agile manner while minimising data loss and downtime will be a strategic priority for many of the Irish banks and financial institutions in 2024. The EU Digital Operational Resilience Act (DORA) is aimed at strengthening the IT security of financial entities such as banks and ensuring that the financial sector in Europe remains resilient in the event of a severe operational disruption. It includes a requirement for control and oversight of third parties managing and supporting critical services for all Irish banks and their affiliates.

2023 has brought with it a wave of new regulations to be applied to the Irish financial sector, such as NIS2 (the Network and Information Security Directive of the EU), and more regulation in the form of the EU AI Act and other pieces of legislation are on the way. Therefore, financial institutions must be ready to face new challenges in adapting their security measures to a continually evolving regulatory landscape.

This will necessitate a realignment of cybersecurity priorities as well as increased resource allocation. Banks will need to be capable of embracing new technologies while ensuring dependable security in an ever-evolving threat environment.

As a result of ongoing geopolitical conflicts in Europe, threat actors will likely keep targeting essential banking infrastructure, making the Irish banking sector vulnerable to distributed denial of service (DDoS) attacks. DDoS attacks were initiated by Russian hacktivists against Czech institutions and the Czech stock exchange. The hackers denied clients of online banking access and demanded that the financial institutions cease their support for Ukraine. In retaliation for Europe's continuous support of Ukraine, several European banking institutions, including the European Investment Bank, were targeted by pro-Russian hacktivists by DDoS attacks in 2023.



Cybersecurity and AI

The implementation of AI in the Irish financial sector gives rise to a number of concerns regarding the inherent risks of the technology. Privacy lapses, a lack of transparency regarding the generation of outcomes, robustness concerns, cybersecurity vulnerabilities, and the influence of AI on overall financial stability are among these issues. However, generative AI could also enhance cybersecurity defences through the implementation of predictive models that identify threats and facilitate incident response.

As large language models (LLMs) become increasingly interconnected with other digital and physical assets within the Irish financial sector, there is a possibility that hackers could devise novel methods to compromise them. These include a technique known as "prompt injection attack," which can get around generative AI's rules and filters or even add harmful data or instructions.

AI is also being used to create more sophisticated phishing messages and emails and to allow criminal actors to assume the identities of individuals or organisations, raising the risk of identity theft or deceit. Deepfakes, which create authentic-looking films, audios, and photos, can also harm Irish financial institutions and individuals.

AI and machine learning systems raise a number of privacy issues that need to be addressed before they can be used in the heavily regulated Irish financial industry. Some challenges that might arise are leaks from the datasets used to train the systems, the ability to figure out anonymised data through predictive analytics, and AI/ML "remembering" information regarding individuals in the training dataset even after the data has been utilised and discarded. These worries are at the core of ongoing efforts to improve the laws and rules that require AI/ML systems and the data sources that go with them to meet higher privacy standards.

Irish firms within the financial sector using public generative AI systems face many privacy challenges. Generative AI systems train and improve their responses by automatically "opting in" users. This increases the risk of the system obtaining financial and personal data from Irish citizens. Indeed, several generative AI systems state that they can't guarantee user data privacy.

Therefore, AI security governance models will have to be developed to answer some important questions: Which roles within engineering, compliance, and security teams within the Irish financial institutions govern AI security? Where do the existing security tools fall short? What does LLM security look like?

Instant Payments

With recent legislative agreement between the European Commission and Parliament, instant payments are now a key focus area for banks. Irish banks will need to offer 24x7 payments which are processed within 10 seconds. Proposed timelines for compliance are nine months for incoming and 18 months for outgoing payments once the legislation is signed off.

This will impact on the way the banks process payments today with knock-on effects across technology, operations and pretty much every aspect of the organisation. Banks will also have to offer Confirmation of Payee services to the customers.

Irish banks are currently in the process of mobilising project teams to meet the new requirements. While many of the banks already have the solution required to implement instant payments, challenges remain due to the legacy infrastructure involved in payments processing. Existing core banking systems are not available 24x7 forcing banks to explore alternate options like stand-in capabilities which are very complex operationally.

Banks that do not have the solutions in place have embarked on a journey to procure a new solution. Banks are also exploring their best option to offer Confirmation of Payee solutions to the customers.

Instant Payments will require stronger and more proactive management of financial crime risk since the ability to monitor risk as part of the payments process will be limited. The Central Bank of Ireland (CBI) has communicated an expectation of a more effective and tailored risk-based approach from payment providers. The regulator has called out common gaps and weaknesses identified when they test compliance frameworks, including inappropriate application of Simplified Due Diligence, and ineffective ongoing monitoring of risk. It is likely that AI and ML technologies will need to be adopted by banks to support more effective transaction screening and monitoring.

Regulatory Change in Payments

We are entering an era of an ever-increasing regulatory burden on the financial services sector. Upcoming changes which will have significant impacts include Payment Services Directive 3 (PSD3), The Financial Data Access Regulation and the Digital Euro.

The EU has introduced a legislative package to modernise and harmonise the existing payments regulatory framework, in light of accelerating innovation and digitisation. The proposals include measures to level further the playing field between banks and non-bank payment providers by making those providers eligible for direct access to all EU payment systems and reinforcing their rights to open and maintain bank accounts.

The package aims to enhance the resilience of the payment sector through stricter safeguarding and wind-down planning requirements. Regulators may also require payments firms to create a separate legal entity for that activity, if they are part of a group undertaking non-payment activities which are likely to be unregulated.

The package also includes proposals to strengthen fraud and consumer protection. These include mandatory free of charge payee verification services, broadening consumers' refund rights for new types of frauds, and providing a robust legal basis for firms to share fraud-related data voluntarily.

If adopted in its current form, the legislative package will bolster the EU payment sector's resilience and competitiveness. However, compliance, including re-authorisation requirements, will demand considerable investment and effort from firms. Given the scale of the ambition and technical complexities involved, final proposals are unlikely to emerge before late 2024 at the earliest.

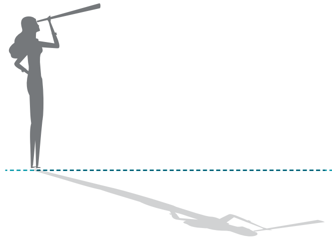
Talent

The impact of generative AI, industry convergence, open data, decarbonisation and sustainability, digital identity, and fraud will grow in 2024. As a result, competition will remain intense for talent for core skills across the three lines of defence. The ability to attract, retain and retrain personnel with these skills will be a critical success factor for banks in 2024 and beyond.

Summary

2024 will present both challenges and opportunities for the Irish banking industry. The onus is on traditional Irish banks to adapt to the digital age and compete with agile fintech start-ups, but they have advantages in the form of their established customer base, brand recognition, and regulatory expertise. By embracing technological innovation, and putting customers to the fore, Irish banks can position themselves for an era of growth by delivering enhanced services and experiences that meet the evolving needs of their customers.

For global insights please read the Deloitte 2024 banking and capital markets outlook.



Contacts

Sean Smith
Partner, Risk Advisory
Banking and Capital Markets Lead
seansmith1@deloitte.ie

Orlagh Tuite
Partner
Consulting, Financial Services
otuite@deloitte.ie

Sinead Moore
Partner
Audit & Assurance
simoore@deloitte.ie

Vaibhav Malik
Partner
Risk Advisory
vaimalik@deloitte.ie

Deloitte.