Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Central Bank of Ireland
Regulatory & Supervisory Outlook

February 2026

Contents

Back to “Contents”

Foreword

I am delighted to introduce the third edition of our Regulatory & Supervisory Outlook setting out our outlook and priorities for the financial sector in the face of a rapidly changing international environment characterised by geopolitical tensions, trade fragmentation, technological disruption and climate transition.

As outlined in my recent letter to the Tánaiste and Minister for Finance, the financial sector has demonstrated its financial and operational resilience through the turbulence of recent years and the technology-driven transformation underway.[1] This is testimony to the adaptability of the sector as well as the solid foundations built since the global financial crisis. As a globally significant financial centre, the firms based in Ireland play a pivotal role in meeting the financial needs of consumers and businesses and the functioning of both the domestic and the European economy.[2]

The question is no longer whether change will come, but the nature, degree and speed of that change and how we respond collectively. Resilience, adaptability and trustworthiness are the qualities that must define that response.

However, there is no cause for complacency given the need to keep pace with a complex and fast-moving external environment and the big structural transformations underway.

Heightened geopolitical and geoeconomic policy uncertainty means risks once considered remote have become more likely, and consumer needs and expectations are changing rapidly. The pace of change and the complexity we face, require adaptability and flexibility to address known or emerging weaknesses in a timely way. The question is no longer whether change will come, but the nature, degree and speed of that change and how we respond collectively. Resilience, adaptability and trustworthiness are the qualities that must define that response.

The purpose of the Regulatory & Supervisory Outlook

It is against this backdrop that this year's Regulatory & Supervisory Outlook (RSO) is published. In January I set out for the Tánaiste and Minister for Finance our views on the economic outlook and our regulatory priorities for 2026. Further to that letter, this document sets out for the benefit of the Central Bank's various stakeholders our latest view of how the accelerating changes in the global

[1] Central Bank of Ireland (January 2026), *Letter to the Tánaiste and Minister for Finance*.
[2] The Central Bank's mandate covers more than 3,300 firms across a range of sectors and approximately 9,100 investment funds. In this report, the terms "regulated entities", "firms" and "institutions" are used interchangeably.

Back to "Contents"

environment are shaping the risk landscape domestically and internationally and the key vulnerabilities we see across the sectors and firms we supervise.

We draw out our assessment of the most consequential risk areas and the resulting activities we plan to undertake over the coming year in response. Our priorities are aligned with those of the European System of Financial Supervision and ECB Banking Supervision.

Our outcomes-focused, risk-based approach to supervision means that we focus our efforts on those risks and vulnerabilities that, in our judgement, pose the greatest threat to the achievement of our four safeguarding outcomes: the protection of consumer and investor interests, the safety and soundness of regulated entities, the integrity of the financial system and financial stability.

As outlined in the RSO, operational and cyber risks remain a key concern given rising risk and threat levels. As such, there will be a significant focus again this year on operational resilience given its critical importance. How firms are securing their consumers' interests in this rapidly changing world, and how they are responding to technological change, are also key priorities.

In 2026 we will also continue to build on the progress we have made in recent years to increase the efficiency and effectiveness of our regulation and supervision. This includes continuing to embed our integrated supervisory approach, continuing to improve our gatekeeping processes and delivering the roadmap of initiatives we set out at the end of last year in our *Regulating and Supervising Well – a more effective and efficient framework* publication.[3]

Gabriel Makhlouf

Governor

26 February 2026

[3] Central Bank of Ireland (December 2025), *Regulating and Supervising Well*.

Back to "Contents"

Executive Summary

Introduction

The 2026 Regulatory & Supervisory Outlook is published at a time of accelerating change in the global environment. Geopolitical fragmentation, macro-financial uncertainty, rapid technological transformation, and evolving consumer needs and expectations are reshaping the financial system and the risks it faces. These developments present opportunities but can expose vulnerabilities, requiring firms and supervisors alike to remain vigilant, resilient and forward-looking.

Ireland's financial sector has demonstrated strong financial and operational resilience through recent economic, financial and geopolitical turbulence, and through an extraordinary period of technology-driven transformation. This resilience reflects both the adaptability of firms and the strong regulatory and supervisory foundations established since the global financial crisis. However, Ireland's position as a highly interconnected financial centre means that risks can emerge and spread quickly. Firms must therefore ensure that they are resilient, well-governed and capable of managing evolving risks in a way that protects consumers and investors, safeguards financial stability and maintains trust in the financial system.

Ireland's financial sector has demonstrated strong financial and operational resilience, but risks can emerge and spread quickly.

The global and domestic risk environment

The global environment remains uncertain and subject to heightened geopolitical and macro-financial risks. Increased geopolitical tensions, economic fragmentation and shifts in global supply chains continue to influence financial markets and economic activity. Changes in market sentiment or macroeconomic conditions could affect stretched asset valuations, liquidity and the resilience of firms and markets.

Technological innovation continues to change financial services, creating efficiencies, supporting innovation and improving customer experiences. However, increasing reliance on digital infrastructure, cloud services and third-party providers also introduces new vulnerabilities, including cyber risks, operational risks and concentration risks. The expanding use of artificial intelligence, digital money and tokenisation presents further opportunities but also requires robust governance, risk management

Back to "Contents"

and oversight to ensure that risks are appropriately managed and consumer interests are protected.

At the same time, longer-term structural transitions, including the transition to a more environmentally sustainable economy, adaptation to increased climate risk, demographic changes and evolving consumer needs, are reshaping the financial landscape. This backdrop informs the risk assessment and outlook set out in Section 2, with ten key risk areas being highlighted grouped into three broad risk driver themes:

Drivers: Macroeconomic and geopolitical environment. Covers operational and cyber risks, and financial risks including credit, liquidity, leverage and market risks.

Drivers: How regulated entities are responding to today's changing world: Includes consumer and investor detriment risks, data, AI and modelling risks, financial crime, and risk management practices.

Drivers: Longer-term structural forces at play. Includes climate risks and business model and strategic risks.

The Central Bank's assessment is that operational risks remain at a very elevated level given the current geopolitical context, advancing digitalisation and increasingly complex operating models. Asset valuation and market risks are judged to have increased, as have the risks associated with data, models and AI. Inflation and interest rate risks have abated.

Supervisory priorities

The Central Bank's supervisory priorities for 2026 address the most material risks facing the financial system and support the delivery of our safeguarding outcomes: the protection of consumer and investor interests, the safety and soundness of regulated entities, the integrity of the financial system and financial stability.

We have five overarching priorities this year:

Priority 1: Maintaining and building resilience to geopolitical risks and macro-financial uncertainties involving work on operational resilience, cyber security and financial resilience in the face of a volatile macro-environment and how firms are embedding climate and

Back to "Contents"

environmental factors into risk management, business models and governance.

Priority 2: Securing consumer and investor interests in a rapidly changing world with a particular focus on a) how firms operate and the customer experience, b) digitalisation, including balancing the benefits of innovation with risks of harm to consumers, and c) financial crime, with rising risks to consumers from frauds and scams.

Priority 3: Responding to technology-driven transformations with a focus on the expanding use of AI, digital money and tokenisation, including our regulation and supervision of the use of these technologies and innovations, and the implications of these changes for firms and the financial system.

Priority 4: Helping to address the environmental and societal transitions underway. Given the impact of these longer-term structural transitions, we will continue to work in partnership with other stakeholders to help address them. This includes work on protection gaps, retail investment participation, the evolving payments landscape and sustainable finance.

Priority 5: Enhancing how we regulate and supervise. 2026 will see a continued focus on evolving our supervisory approach to ensure its continuing effectiveness, improvements to gatekeeping and the roadmap for delivering on simplification as set out in our recent "*Regulating and Supervising Well*" publication.

Looking ahead

The Central Bank will continue to be outcomes-focused, risk-based and forward-looking ensuring we remain effective in addressing the rapidly changing risk landscape. Firms are expected to maintain strong governance, risk management and operational resilience, and to act in the best interests of their customers.

Back to "Contents"

Box 1: Overview of the RSO

Section 1 describes the global macro environment, major trends and drivers of risk.

Section 2 outlines the Central Bank's assessment of the key risks facing the entities we regulate and the consumers and investors whose interests we seek to protect.

Section 3 covers the Central Bank's overarching supervisory priorities in the context of the safeguarding outcomes we seek to achieve.

Section 4 provides a sector-by-sector view, including the key areas of supervisory focus and planned activities.

The RSO also features three articles addressing specific topics in more detail:

- ***Spotlight 1*** provides a supervisory perspective on artificial intelligence.
- ***Spotlight 2*** covers the importance of operational resilience in service provision, which is a key focus of our work.
- ***Spotlight 3*** describes our approach to consumer and investor protection and three high level outcomes-focused themes.

The RSO sits alongside the Central Bank's publications that have a macroeconomic or financial stability perspective, notably the biannual Financial Stability Review (FSR).[4] The FSR focuses specifically on risks facing the financial system as a whole and the resilience of that system. The scope of the RSO covers broader dimensions including the interests of consumers and investors, the safety and soundness of regulated entities and the integrity of the financial system.

[4] See Central Bank of Ireland (November 2025), *Financial Stability Review 2025:II*.

Back to "Contents"

Section 1 – The Global Macro Environmental Drivers of Risk

Introduction

This section provides a high-level overview of the major developments and trends we see in the global macro environment that create both risks and opportunities within the financial system domestically and internationally.

Politics and geopolitics

Geopolitical shifts are fracturing the global order heightening uncertainty and increasing security risks. The past year has seen further moves towards protectionism and weakened international cooperation as some countries prioritise a more unilateral approach to protecting their economic, security and strategic interests. While the impact of US tariff policies has so far been less severe than initially feared, the Irish and global economy is still adjusting to the new trading environment and policy uncertainty remains heightened. Instability is exacerbated by the ongoing war in Ukraine and the other conflicts and tensions around the globe.

The geopolitical and security developments seen in recent months have highlighted that Ireland faces specific risk drivers and vulnerabilities. These arise from the country's position as a small, open economy with a very large, internationally connected financial sector and include, amongst others, system-wide operational risks. For example, Ireland hosts a significant share of EU's data subsea cables.[5] Infrastructure vulnerability could raise concerns about the operational resilience of the financial system and firms.

Financial and macroeconomic conditions

The global and domestic economies have demonstrated resilience to date, but uncertainty remains high and the outlook is tilted to the downside. Shifting trade policies continue to weigh on global economic activity. Going in the other direction, investment in AI and related infrastructure is providing a tailwind to growth, especially in the US. Inflation in the euro area fell back to target during 2025 while

[5] Government of Ireland (December 2019), *National Cyber Security Strategy 2019-2024* and Centre for Strategic and International Studies (July 2025), *The Strategic Future of Subsea Cables: Ireland Case Study*.

Back to "Contents"

the return to target is expected to be more gradual in the US. The global economic outlook is tilted to the downside, stemming from a potential further escalation of trade tensions, a crystallisation of geopolitical risks, or a reassessment of expectations around the effects of AI on productivity growth. Domestically, the outlook is also tilted to the downside, with Ireland particularly exposed to further shifts in the international trading and investment environment. Downside risks could also arise if there were delays in delivering critical infrastructure, such as housing, transport and energy, constraining the economy's growth potential.

Financial markets generally had a strong year in 2025 and the start of 2026 despite the uncertain backdrop, driven largely by AI-based growth expectations and compressed corporate bond spreads. High valuations are a possible sign of excessive risk taking (with "fear of missing out" being one driver) increasing the risk of market corrections, particularly in relation to AI-driven valuations, albeit with the timing uncertain. The increased presence of non-bank financial intermediaries (NBFI) in financial markets – where associated with underlying financial vulnerabilities – could amplify risks in unanticipated ways in the event of a significant stress event or sudden change of sentiment.

Technology and innovation

Advancing digitalisation and changing consumer expectations are reshaping the nature, form and delivery of financial products, creating both opportunities and challenges. Many of the more recent technological innovations, such as tokenisation and stablecoins, have the potential to reshape finance for the better through operational efficiencies and improved financial offerings. But they also entail risks that need to be managed and raise environmental concerns. Specific products enabled by this new technology, such as crypto, elevate fraud and financial crime risks, and could, over time, increase financial stability risks as they become a more material and integral part of the financial system.

Advanced AI tools offer the potential for greater productivity, improved investment performance, more tailored products and services, and better risk management. However, the risks of bias, misinformation, data loss and a "black box" lack of transparency create vulnerabilities and require vigilance. The wide availability of GenAI is also making it easier for criminals to conduct illicit activity and perpetrate fraud. This is not because the technology is inherently

Back to "Contents"

bad, but because it lowers technical barriers and increases the scale, speed and realism of attacks. In early 2025, AI-supported phishing reportedly made up over 80% of such activity globally.[6] AI tools, however, can also assist in the fight against financial crime.

Spotlight 1 - Approaching AI from a Supervisory Perspective reviews trends in the technology itself and its adoption.

Climate and the environment

The risks associated with the climate and environmental crises are becoming more evident. Extreme weather events such as floods, storms and wildfires are increasing in frequency and severity, impacting national and regional infrastructures, businesses, households and ultimately could affect the creditworthiness of some financial counterparties and collateral values while heightening operational risks. If action is delayed - and if transition financing and delivery remains inadequate - the chances of a disorderly transition, with more material or abrupt future policy changes and potential sharp market adjustments, could increase.

The rapid loss of species, ecosystems and other natural resources upon which human wellbeing is dependent is becoming recognised as a driver of risks to public health, the economy and, through that, the financial system. For the financial sector that can translate into economic, credit, market and insurance risks as enterprises dependent on healthy ecosystems face potentially reduced productivity, higher costs and asset impairment.

Social and demographic

Social and demographic trends are likely to have significant effects on the financial services landscape, including the types of products consumers need, structural implications for savings and investments, and the risks of protection or savings gaps. Younger, digitally native individuals tend to expect low-cost, real-time and increasingly personalised services, with some also having a high enough risk appetite to consider investments and advice from providers and influencers outside the traditional regulatory perimeter. Ageing populations across Europe increase the requirement for mainstream pensions savings vehicles, retirement income products, healthcare and long-term care financing, placing pressure on public finances where these are provided by the state.

[6] ENISA (October 2025), *Threat Landscape report 2025*.

Back to “Contents”

The new Irish auto-enrolment pension scheme "My Future Fund", the government's National Financial Literacy Strategy and Europe-wide initiatives to increase retail investment participation are efforts to address some these challenges. Policymakers, regulators, financial services firms and other stakeholders all have an important role to play in ensuring these positive initiatives are designed and delivered in a way that secures the best interest of consumers, investors and the wider economy.

Legal and regulatory

There has been a significant recent shift in the global regulatory environment, with fragmentation and localisation creating a more complex operating environment for globally active firms and variability of regulatory standards. Such fragmentation is seen particularly in the digital assets, AI and climate spaces, with diverging approaches emerging in major jurisdictions. This comes in the context of a financial system which continues to become increasingly internationalised, interconnected and reliant on internationally available technologies and providers. The fragmentation of rules on which an interdependent global financial system relies presents clear risks. In the EU, while simplification of EU regulation is needed, there is a risk that it also leads to inadvisable deregulation and repeating past mistakes.

Further detail on key EU and domestic regulatory initiatives is set out in Appendix A.

Navigating the future

Navigating the rapidly changing environment requires looking ahead, with a clear focus on the fundamentals of finance: sound governance, effective risk management and financial and operational resilience. A confluence of events or change in sentiment can lead to severe and sudden disruptions with far-reaching consequences for economies, financial markets, firms and consumers. The consideration by firms and regulators alike of the "tail risks" associated with very low probability but ultra-high impact events (possibly occurring at the same time due to known and unknown interconnections) is becoming more crucial.

In the 2025 RSO, we highlighted the importance of using scenario analysis and understanding transmission channels to help navigate

Back to "Contents"

this environment. [7] Such analysis complements and builds on traditional stress testing methods and crisis simulation exercises that are routinely used by firms and supervisory authorities to test financial and operational resilience and to identify vulnerabilities (and opportunities).

Appendix B reproduces the stylised diagram we used to illustrate the varied and complex channels at play.

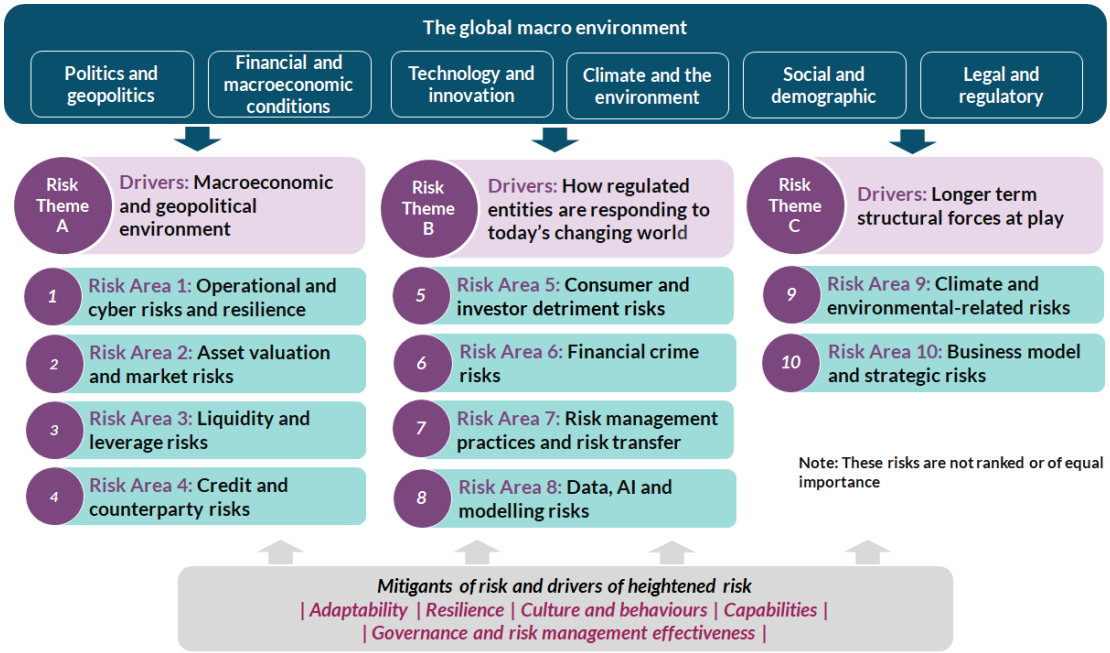
[7] See Spotlight 3 of Central Bank of Ireland (February 2025), *Regulatory & Supervisory Outlook*.

Back to "Contents"

Section 2 - Risk Assessment and Outlook

In the context of the complexity and uncertainty evident in the global macro environment and described in Section 1, this section sets out our assessment of the key risk areas facing the financial sector which has informed our supervisory priorities. They are grouped into three themes as shown in Figure 1: risks driven by the macroeconomic and geopolitical environment, risks driven by how regulated entities are responding to today's changing world and those driven by the longer-term structural forces at play.

Figure 1 – Overview of Risk Themes and Key Risk Areas

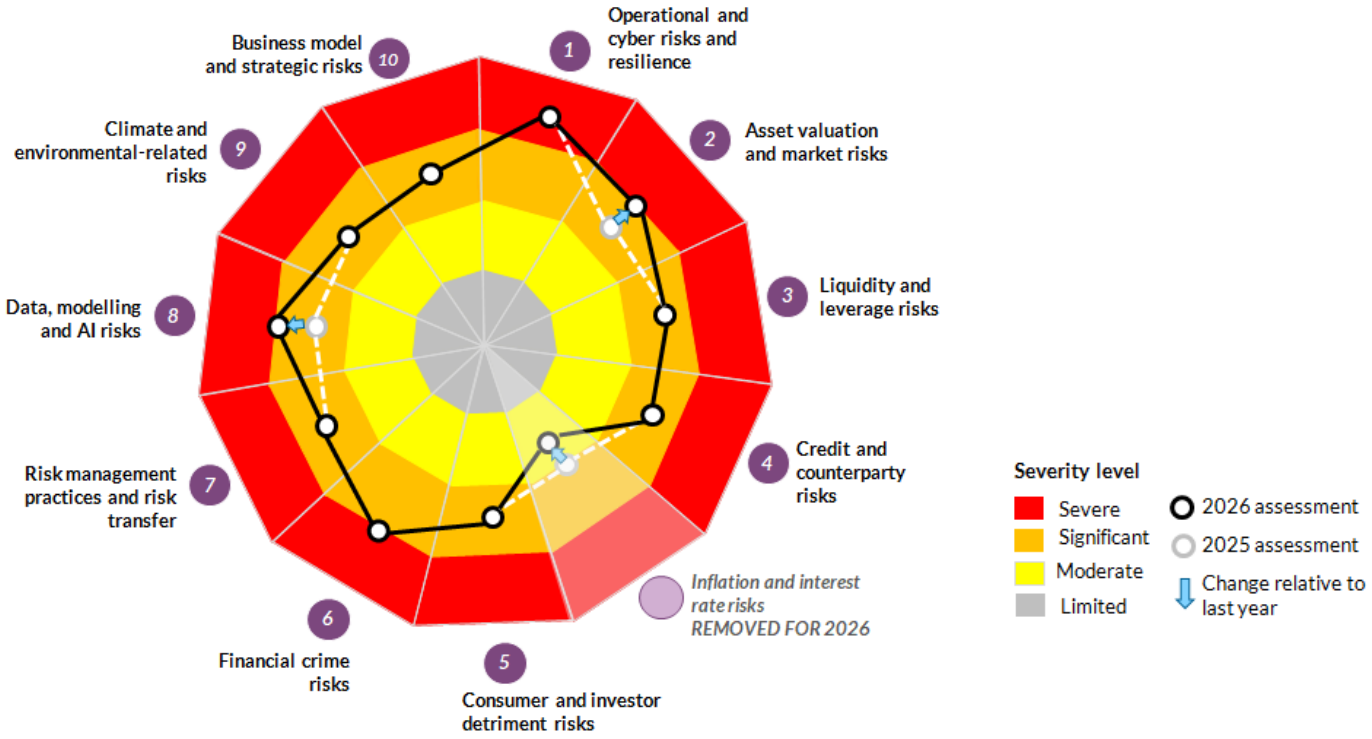


Our latest assessment of the risk severity level for each risk area and the movements from last year are shown in Figure 2.

Inflation and interest rate risks featured as a key risk area in the 2024 and 2025 RSOs but has reduced to a moderate assessment, based on which we have removed it from the list of key risk areas; however, it remains an area for vigilance and features within other risk areas. The reduced risk rating reflects both the evolution of inflation dynamics – and the current stance of monetary policy in the euro area - as well as the fact that regulated entities with greatest exposure (for example, banks and insurers) have been strengthening their management of these inherent risks, their resilience and the supports provided to affected consumers.

Back to "Contents"

Figure 2 – Risk radar showing the assessed risk severity level and change since last year[8]



The assessments of each risk area and supporting commentary set out in Table 1 aim to draw out relativities between the risk areas and trends over a two-year horizon. The assessments reflect the regular sectoral assessment of risks we undertake as part of our approach to supervision, a "top down" holistic view, and are also informed by the risk assessments undertaken by the European Supervisory Authorities (ESAs), ECB Banking Supervision and other international bodies.

[8] Appendix C provides a description of each risk severity level.

Back to "Contents"

Table 1 – Risk assessment overview

Risk Theme A: Risks that are predominantly driven by the macroeconomic and geopolitical environment

1. Operational risks and resilience

Since last year → Outlook ↗

Increased geopolitical fragmentation and operational complexity raise the likelihood of cyber and other disruptive events, compounded by the rapid rise in cloud computing and growing reliance on a small number of technology providers and infrastructure for critical services.[9] Combined, these raise both the probability and potential severity of accidental or malicious incidents as well as the speed of system-wide transmission, with detrimental effects on users.

Cybersecurity threats are intensifying due to AI advancement, geopolitical fragmentation and complex supply chains, creating a landscape where the speed and scale of attacks can exceed traditional defences. While AI strengthens both defensive and offensive capabilities, organisations may struggle to balance innovation with security as governance and risk management try to keep pace with technological developments.[10]

Spotlight 2 – Supporting Resilient Service Provision provides additional context to the supervisory activities and expectations linked to the Digital Operational Resilience Act (DORA).

2. Asset valuation and market risks

Since last year ↗ Outlook ↗

Equity and debt valuations are stretched despite geopolitical uncertainty. Investor sentiment could shift quickly with ever faster speed of transaction execution, increasing market volatility and downside risks. Ongoing concerns about the opacity and reliability of some valuations, notably in private credit and private equity, increase risk levels.

Valuations for AI-related stocks or firms expected to benefit from the implementation of AI, as well as associated debt instruments, are particularly vulnerable to any marked change in attitudes to the multi-billion- dollar investments being made and expectations around the speed or success of AI adoption. Similarly, sectors set to lose out from the adoption of AI may experience volatility. The high concentration of AI-related stocks in US equity markets amplifies revaluation risks.

3. Liquidity and leverage risks

Since last year → Outlook →

Liquidity and funding positions across sectors remain healthy overall, but pockets of high leverage and/or asset holdings that may have low liquidity in certain situations (e.g. relating to private credit, private equity, infrastructure or real estate) can amplify market stress. Swiftly changing sentiment can lead to bank deposit withdrawals (that are now instantly executable) and dashes for cash from open-ended funds, stablecoins and other structures that have liquid liabilities.

The NBFI sector has grown substantially over the past decade to represent nearly half of global financial assets, increasingly employing leverage through debt, repurchase agreements, securities financing transactions or synthetic means (e.g. via derivatives). High leverage or liquidity mismatches in NBFI can create significant financial stability risks, particularly when concentrated in entities that are key participants in systemically important markets. In addition, the

[9] On cloud computing, four US companies hold about 70% of the EU market, with concentrations also to US BigTech on productivity tools and software and consumer platforms. Source European Parliament (December 2025), *European Software and Cyber Dependencies*

[10] World Economic Forum (January 2026), *Global Cybersecurity Outlook 2026*.

Back to "Contents"

interconnectedness of NBFI with other financial institutions including banks, can act as a further source of spillovers of shocks.

4. Credit and counterparty risks

Domestic borrowers have largely remained resilient to economic shocks and interest rate increases in recent years, but downside risks remain amid heightened geopolitically driven volatility which could potentially lead to increased defaults over time. Internationally, there are concerns around lending standards and a lack of transparency in global private credit markets, as well as the expanding role and interconnectedness of NBFIs, potentially amplifying risks in unforeseen ways during periods of market stress.

Earnings and repayment capacity of some borrowers could be impaired by macroeconomic shocks, including tariffs, but other elements of geopolitical risk such as cyber-attacks can also threaten counterparties' financial health.

Risk Theme B: Risks that are predominantly driven by the way regulated entities operate and respond to the evolution of their marketplace and today's changing world

5. Consumer and investor detriment risks

Evidence persists that some firms are not sufficiently consumer centric, causing actual and potential harm due to, for example, a lack of transparency on product risks and charges (including unregulated products), possible conflicts of interest and insufficient focus on customer financial wellbeing, service and access.

Digitalisation and innovation are also key factors, amplifying both opportunities and risks for consumers and investors, especially for those in or facing vulnerable circumstances.

6. Financial crime risks

Financial crime risks span money laundering, terrorist financing, sanctions breaches, market abuse, fraud and unauthorised services. There is an increased exposure due to the shift to digital-first financial services and crypto-assets which have specific vulnerabilities to financial crime. Money laundering is increasingly driven by sophisticated threat actors operating across borders while traditional terrorist financing and sanctions evasion threats remain.

The increasing volume of unauthorised activity, financial scams and fraud is being driven by technology which is providing criminals with new and innovative ways to harm consumers. Digitalisation which facilitates instant payments, e-money and crypto plus new AI tools, expands perpetrators' capabilities and opportunities. This is compounded by weak controls in some firms, with heightened risk of exploitation across channels and products, including cross border.

7. Risk management practices and risk transfer

Firms increasingly transfer risk (e.g. credit, market, insurance/longevity) to manage exposures and/or to optimise capital and rates of return. While beneficial, this can increase cross-sector and cross-border linkages, creating potentially hidden concentration and counterparty exposures, and – if it amounts merely to regulatory arbitrage - may reduce the total capital held across the system against unchanged aggregate risk.

Synthetic risk transfer transactions can facilitate increased leverage and may require frequent rollovers (leading to rollover risk) and could potentially undermine risk transfer if not properly managed or adequately collateralised. In addition, there is the potential risk associated with a

Back to "Contents"

concentration of synthetic risk transfer counterparties. This could impair the effectiveness of risk transfer in the event of a deterioration in the financial position of any significant counterparties.[11]

8. Data, modelling and AI risks

Since last year ↗ Outlook ↗

Advanced models and expanding data collection have long been used by leading firms, but widespread adoption of third-party AI tools changes the risk landscape and calls for stronger model governance, data quality, transparency and accountability. AI can amplify existing weaknesses, with model risk a growing concern in a world where the future differs from the past and is more unstable, and as models drive more business decisions in more firms. AI developments also heighten operational risk, business model risk, and risks to consumers.

Box 2 – Data Quality and Effective Data Management Practices covers the findings of the Central Bank's supervisory work in this area and the implications for firms.

Risk Theme C: Risks that are driven by the longer-term structural forces at play

9. Climate and environmental-related risks

Since last year → Outlook ↗

The Irish financial sector's international footprint means extreme weather events can impact firms' commercial, operational, counterparty and insurance risk exposures both abroad and at home. The economic and financial costs of climate change are already materialising. A quarter of all weather and climate-related economic losses in Europe since 1980 occurred in the past four years. In Ireland, Storm Éowyn resulted in over €300m in insurance claims, the most expensive insurance event related to storms in Irish history. Delays in taking the required climate mitigation actions globally increase the likelihood of a disorderly transition and amplified physical damage.

Changes to EU regulations on sustainability related disclosures will limit the data available to both manage risks within the financial system and identify opportunities to support the transition to net zero. Heightened risks remain to consumers and investors from firms overstating green credentials (greenwashing), which also undermines the effective financing of the transition and climate adaptation.

10. Business model and strategic risks

Since last year → Outlook ↗

Digitalisation (including tokenisation and stablecoins), geoeconomic fragmentation and demographic shifts, evolving consumer needs and new international competition may challenge the long-term sustainability of some firms, potentially including critical service providers. Firms may fail to manage the development of their business model or strategies in a way that is consistent with our safeguarding outcomes.

While competition from overseas, agile specialists and Big Tech may improve choice, it can – as it has in the past - trigger a race to the bottom in decisions, heightening the risk of disorderly market exits. The many firms in Ireland that are subsidiaries of global organisations are also exposed to changes in the strategy being pursued by their parent which may see their role in the group change with little notice.

[11] ESRB (May 2025), *Unveiling the impact of STS on-balance-sheet securitisation on EU financial stability*.

Back to "Contents"

Addressing the risks associated with long-horizon structural transitions

In addition to those set out above, certain risks to our safeguarding outcomes accumulate gradually and may not be captured through cyclical or firm-level supervision. These cover the long-horizon structural transitions and risks arising from demographic, economic, societal and environmental changes that may crystallise into consumer harm or financial instability over time.

While the immediate risk may be low, inaction now would have significant long-term consequences. Understanding and addressing these challenges requires many stakeholders to act, including the Central Bank and regulated financial institutions.

Mitigants of risk and amplifiers of risk

As noted in previous RSOs, across all the risk themes described above, a risk mitigant is that a firm has a culture and approach that supports the management of its operations in a prudent, proper, forward-looking and consumer-centric way. This includes having the expertise, experience, infrastructure and governance structures in place to run it well. Assessing how firms are managing these endogenous mitigants and amplifiers of risk within their organisations is a core element of our supervisory work.

The key risks outlined above provide the backdrop for the Central Bank's supervisory priorities for the period ahead and inform our supervisory focus. Section 3 explains the Central Bank's overarching supervisory priorities, with Section 4 providing a sector by sector view.

Box 2: Data Quality and Effective Data Management Practices
Lessons from the Central Bank's Thematic Work and Deep Dive Inspections

Background: Data quality covers the accuracy, reliability, completeness and consistency of information. It affects all activities within a firm ranging from risk management, strategic decision making, product design and pricing to regulatory compliance and beyond. Data inaccuracies, staleness and gaps can undermine the integrity of firms, the financial system and the effectiveness of supervision. The quality of data should be of particular concern for senior executives as it can directly impact their ability to make informed decisions. Data quality, therefore, is an enduring supervisory focus. With the exponential growth in the volume of internal and external data that firms process and

Back to "Contents"

use, plus the growing use of advanced models for decision making and the deployment of AI tools, sound data management practices are more crucial than ever.

Understanding the root causes of deficiencies: It can be easy to label weak systems, weak policies and weak frameworks as the primary causes of poor data quality. However, from our work, we find that there are often several factors which combine to feed into and perpetuate data issues. Some root causes may be structural, for example poor data governance practices or an insufficiency of resources, but these can be compounded by behavioural factors. Poor organisational culture may mean that staff do not feel they can highlight data sets they believe to be inaccurate or model output that has material limitations. If staff do not feel safe, data risk can accumulate silently. It follows that by only concentrating on IT deficiencies, data quality problems are unlikely to be fully and sustainably resolved. Comprehensive remediation requires all aspects to be tackled holistically.

Addressing data quality issues and data errors: Data quality can be improved and maintained in the long term by integrating sound error management into a firm's culture and ways of working. Good data practices require clear responsibility and accountability for data governance, with fit for purpose and rigorously tested systems of controls. Open sharing of lessons learned is required, with thorough root cause analyses which do not simply stop at "human error" or "IT constraints". A psychologically safe climate needs to prevail, with the acceptance of "bad news" by leadership and other stakeholders.

Implications for firms: The Central Bank acknowledges that comprehensive remediation of data quality issues and embedding a strong learning culture can be a multi-year and complex undertaking. What concerns us is when firms only engage in short term strategies to firefight immediate issues. This is neither efficient nor sustainable. It is a much better investment of time, money and effort for firms to plan and commit to longer term, fundamental change. Reliable, accurate, complete information supports sound governance, informed decision making and resilient performance which are all essential in delivering better outcomes for consumers and investors alike.

Back to "Contents"

Spotlight 1 - Approaching AI from a Supervisory Perspective

KEY TAKEAWAYS

- As AI capabilities continue their rapid evolution, financial sector deployment is growing. Ireland ranks highly in AI readiness and adoption at a national level, yet public trust is lower than average and adoption rates vary significantly across age demographics.
- AI driven conduct and operational risks require close monitoring by firms and regulators, amid evidence that the safeguards built into providers' AI models can be brittle. Agentic AI's potential is significant but presents one frontier AI risk.
- Geopolitical fractures can jeopardise digital supply chains, including the security and continuity of access to AI models and the technological infrastructure used in financial services.
- Many of the risks associated with AI are not new and are already covered by existing regulations and standards, with the AI Act representing a targeted addition to the operating framework. A focus on the core principles of explainability, accountability, good governance and strong risk management is essential.

Introduction

The Central Bank continues to undertake market monitoring and supervisory risk assessment work relating to the use of AI across the Irish financial sector and internationally. This Spotlight reviews trends in the technology itself and its adoption and considers three aspects related to financial services: the deployment of agentic AI, AI related consumer protection risks and operational resilience.

The technical landscape is extremely fast-moving and complex, with the public's attitudes and engagement evolving. Appendix D provides a summary of some key aspects of the changing landscape for context. It is against this rapidly evolving and transforming set of AI tools that firms, legislators and supervisors must constantly evolve their strategic and practical responses. A focus on the core principles of explainability, accountability, good governance and strong risk management is essential. Technical competence and ethical behaviour are required from those using the tools and

Back to "Contents"

vigilance by those whose wellbeing will be positively or negatively affected by their deployment.

The EU Artificial Intelligence Act (AI Act) that came into force in 2024 is a central framing for how European supervisory authorities view AI use in financial service. The Irish government has designated the Central Bank as a regulator under the AI Act for the financial services under its remit. It is progressing legislation to implement this cross-sectoral regulation in Ireland by August 2026.

The EU Commission proposed a simplification of the AI Act in November 2025. It includes simplifying aspects of related data, cybersecurity and some other specifics. It moves the start date to December 2027 for the application of the requirements for "high-risk" AI systems. High-risk AI systems in financial services primarily include AI used to evaluate creditworthiness, establish credit scores, or assess risk and pricing for life and health insurance. These systems are deemed high-risk because they directly impact individuals' access to essential financial services.

AI is already used across a range of activities

There is widespread adoption of generative AI today with surveys showing that firms expect significant expansion over the next three years. AI use cases include information security and cyber resilience, fraud prevention and detection, customer service via chatbots, supporting coding, pricing and claims underwriting, portfolio optimisation and compliance functions.

Agents are being deployed in some financial services firms' internal operations, but it is not clear exactly how use of agentic AI (AAI) will develop.[12] While it has potential to accelerate beneficial uses of AI through increased flexibility, it adds to system complexity which increases the challenge of understanding and managing risk for both developers and users. Payments via agents may be one of the ways through which agents will be a bridge between the financial system and digital platforms. Several technology firms, payments companies and credit card providers have developed protocols for this type of agent-based transactions.

[12] Agent AI systems are ones that can complete multi-step actions on behalf of users, with varying degree of autonomy using large language models (LLMs) to plan and act within the system. Agentic AI involves setting the goals for a system to achieve and the tools it can use to achieve them but not specifying each step.

Back to "Contents"

There is emerging evidence of use in parts of the European financial sector including cryptocurrency transactions. This means that AAI systems have the potential to complete more financial transactions autonomously within boundaries.[13] At present, the vast majority of transactions are through traditional channels and the regulated financial system. However, the prevalence of this type of activity and the implications for risks to conduct, financial integrity and operational resilience require further monitoring.

In the current geopolitical environment, the resilience of layers of digital supply chains has taken on heightened strategic significance. Disruptions arising from trade or technology restrictions could impair access to critical AI services. Understanding the nature of digital supply chains means looking at the resilience of their underlying layers including models and infrastructure**.** Risk and dependencies on AI and cloud providers from a small number of locations amid geopolitical fragmentation requires firms to consider their contingency options in the event of adverse developments.

Consumer protection risks can be amplified by AI

According to an IPSOS survey, about two in three people globally feel they have a good understanding of AI with a similar percentage in Ireland.[14] However, 46% of surveyed Irish people have concerns relating to AI bias and discrimination, 50% relating to data protection, and 78% supported more transparency relating to AI use in products and services.

Developing robust methods to assess AI related conduct risks and to evaluate the efficacy of safeguards is important, yet this area remains significantly underdeveloped compared to the technology industry's capabilities.[15] To better understand the emerging risks to consumers, the Central Bank will be undertaking further evaluation work in this area and engaging with firms, peer regulators and the European Supervisory Authorities. Box 4 in Appendix D presents results from a risk benchmark study which suggest a wide variation in the effectiveness of the safeguards built into different AI models to refuse harmful requests in a financial services context.

[13] See Figure 23, UK AI Security Institute (December 2025), *Frontier AI Trends Report*.
[14] IPSOS (June 2025), *IPSOS AI monitor 2025*.
[15] The computing and research funding resources available to academic and public interest researchers or public authorities for safety testing are a very small fraction of those of frontier AI companies.

Back to "Contents"

The supervisory perspective

The Central Bank's supervisory approach to AI is consistent with that being taken by the EU AI Office as the lead authority for AI in the EU. Meanwhile, the ESAs are converging around an outcome-focused approach to AI risk-management anchored in the AI Act, DORA, and the existing sectoral regulation and guidance. This focuses on governance, proportionality, accountability and integration into the mainstream prudential and conduct risk frameworks of regulated firms, not treating AI as a silo.

The EU AI Office will play a key role in implementing the AI Act. It will be providing cross-industry guidance on a range of areas relevant to financial services such as the AI system definition, high-risk classification and prohibited practices as well as being a supervisor of frontier AI across the EU.

AI considerations feature in our supervisory priorities as set out in Section 3 and Section 4, with the degree of focus varying depending on AI's significance in each sector, our assessment of risk and the wider European supervisory agenda. Many of the risks associated with AI are not new and are already covered by existing regulations and standards, with the AI Act representing a targeted addition that will need integration into firms' operational frameworks.

Firms must adhere to the following standards when deploying AI:

- **Strategic alignment:** Firms must ensure their use of AI is appropriate for the specific business challenge being addressed.
- **Accountability and explainability:** They should establish clear accountabilities and responsibility, human oversight of decisions and their explainability.
- **Proportionate governance:** Risk management practices must be commensurate with the scale, scope and sensitivity of the AI deployment.
- **Compliance:** Processes should be in place to ensure all EU AI Act obligations are met including transparency requirements.

Back to "Contents"

Spotlight 2 - Supporting Resilient Service Provision

KEY TAKEAWAYS

- The Central Bank's aim is to see firms deliver operationally resilient services to consumers and investors. Designing resilient services means that consumer and investors can have confidence that firms are able to withstand unexpected disruptions or quickly recover to ensure uninterrupted services.
- Effective information and communication (ICT) risk management is core to the delivery of services resilience. The new EU-wide Digital Operational Resilience Act (DORA) went live in January 2025.
- DORA's objectives can be framed around five interlocking aims that, taken together, are intended to drive a customer-oriented mindset focused on maintaining resilient financial services to society.
- There are common gaps in firms' practices when assessed against DORA and firms need to demonstrate that they are systematically addressing those gaps. More generally, firms can significantly enhance resilient delivery of their services in three steps:
    - Identify their critical or important business services to consumers and investors
    - Address the gaps in ICT risk management and operational resilience practices when benchmarked against the good practices outlined in DORA
    - Reflect on significant reliance on third-parties and manage risks proactively.

Introduction

Operational resilience is the ability of a firm and the financial services sector as a whole to identify and prepare for, respond and adapt to, recover and learn from significant unplanned disruptions, while minimising impact and protecting customers and the integrity of the financial system. The provision of effective financial services for consumers and investors is dependent on a resilient system that can maintain critical services – both digital and non-digital – through disruption. Where firms have robust operational resilience capabilities it protects consumers and investors, preserves safety and soundness and limits systemic risk arising from technology

Back to "Contents"

failures or cyber incidents. The first step in becoming operationally resilient is accepting that disruptive events will occur, and that these events will need to be managed effectively.

The introduction of DORA put in place a framework to strengthen the financial sector's resilience to operational disruption, particularly (ICT) risks.

Tackling the key services resilience and ICT risks affecting users of financial services today

Services resilience refers to the ability of any financial services firm to maintain services to end users such as consumers and investors by withstanding unexpected disruptions and recovering quickly. The capability to maintain services through disruption is different to risk management. Effective risk management is how firms reduce the likelihood of disruptive events occurring in the first instance.

EU-wide DORA went live in January 2025. DORA's objectives can be framed around five interlocking aims that, taken together, are intended to support a customer-oriented mindset focused on maintaining resilient financial services to society. To achieve this, firms must identify their critical or important business services (CIBS) to customers and map their ICT risks to their critical service delivery chains. DORA seeks to support this outcome through:

1. **Strengthening ICT risk management across financial entities by instilling good practices:** This requires firms to have clear roles and responsibilities for the management body; comprehensive ICT risk management frameworks that identify, assess, mitigate and monitor ICT risks; integration of ICT risks into business decision-making; and structured governance and reporting lines that make ICT risks visible and addressable.

2. **More effective management of ICT incidents:** This will be demonstrated through improved capabilities for detection, classification, escalation, response, recovery and post-incident learning; timely and accurate incident reporting to competent authorities; and sector-level information sharing to detect, prevent and mitigate emerging threats.

3. **Strengthening the management of ICT third-party risk:** Best practice third party risk management occurs when there is enhanced due diligence, minimum standards in contracts to

Back to "Contents"

ensure resilience, ongoing monitoring, concentration risk assessment and credible exit/termination strategies, recognising that for many firms, ICT risk management is fundamentally a third-party risk management challenge given their scale of outsourcing.

4. **Strengthening the resilience of services provided by critical third-party firms:** EU-level designation and oversight of critical ICT providers to the European and Irish financial systems designed to boost recoverability and resilience standards for services upon which Irish firms depend.

5. **Enhanced assurance of cyber resilience through Threat-led Penetration Testing (TLPT):** A systematic programme that tests firms' defences against realistic threat scenarios, uncovers "unknown unknowns" in critical systems and drives remediation that improves prevention, detection, response and recovery.

The Central Bank is working with financial services firms across the entire financial system to enhance services resilience and meet the best practices required under DORA. Our early observations from engagement across the system is that there are gaps in key areas:

- **Designing and operationalising ICT risk management frameworks**: Most firms have addressed the design aspects of DORA Level 1 and Level 2 requirements through documentation and building frameworks. However, end-to-end embedding in practice is still a work in progress and needs to be addressed with urgency.

- **Strengthening governance and management body oversight:** Firms need to clarify responsibilities and reporting lines and raise ICT risks to board-level attention. Gaps remain in senior management ownership and oversight of ICT.

- **Improving ICT security:** In the context of an evolving threat environment, baseline controls need to be continuously strengthened and policies updated. It is important that firms do so, making part of these enhancements business as usual.

- **Maturing incident management:** Classification, escalation and response processes are being improved, and incident reporting practices are being operationalised. We remain concerned about under-reporting of incidents to regulatory

Back to "Contents"

authorities which may reflect gaps in firms' own internal incident reporting processes.

- **Developing ICT third-party risk management:** Due diligence, contractual controls and monitoring need to be strengthened, with firms increasingly aware of concentration and vendor lock-in risks, and the need for credible exit plans - particularly in cloud and managed services.

The Central Bank's supervisory work on operational resilience in firms supports, and is linked to, broader work of the Central Bank on system-wide operational resilience. This work, in collaboration with industry and government, will explore the ability of the financial system as a whole to continue to provide critical services, such as payment services, in the event of system-wide disruptions.

Conclusion

Services resilience and effective ICT risk management are non-negotiable requirements so that financial services firms deliver on commitments to consumers and investors to maintain their critical services through disruption. This can be achieved in three integrated steps:

- Firms must identify their CIBS to customers and investors and map their ICT risks to these critical service delivery channels.
- Address the gaps in firms' ICT risk management and operational resilience practices when benchmarked against the good practices outlined in DORA.
- Reflect on firms' significant reliance on services provided to them by third parties outside the financial services sector and manage those third-party risks proactively.

Our aim is to see firms deliver operationally resilient services for consumers and investors and raise the level of trust stakeholders have in the financial sector.

Back to "Contents"

Section 3 – Supervisory Priorities

Introduction

The Central Bank's mission is to serve the public interest. We do this through our international and domestic work across our broad mandates. Outcomes-focused, risk-based supervision means that we focus our efforts on those risks and vulnerabilities that, in our judgement, pose the greatest threat to the achievement of our four interconnected safeguarding outcomes: the protection of consumer and investor interests, the safety and soundness of regulated entities, the integrity of the financial system and financial stability.

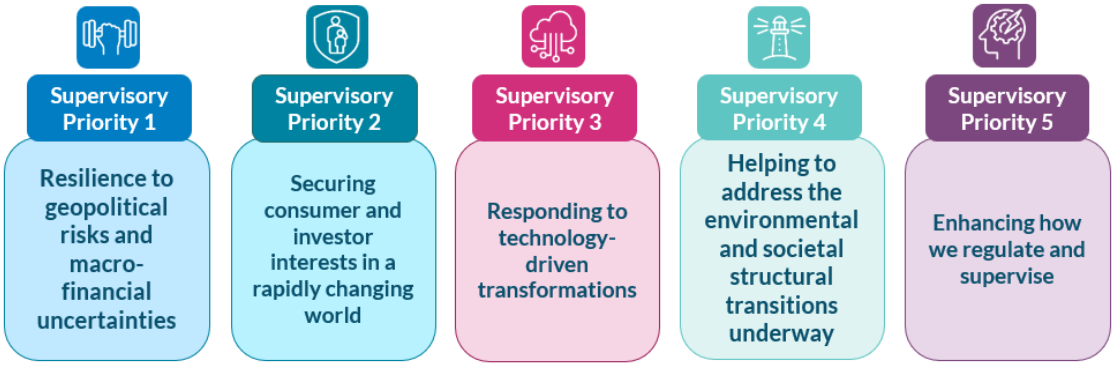
Our supervisory work is undertaken in the context of new legal and regulatory initiatives that have come to fruition in recent years. For example, the Digital Operational Resilience Act (DORA), the Markets in Crypto Assests Regulation (MiCAR), the EU AI Act, the Individual Accountability Framework, the revised Consumer Protection Code, and changes to the lending framework for credit unions. There is a consequent shift of effort to monitoring the embedding of the requirements by firms and the effectiveness of the new regimes in meeting their stated objectives.

Our supervisory priorities

Our priorities for 2026, grouped under five complementary and overlapping themes are set out in Figure 3. These are the framing for the multi-sector and sector-specific work plans outlined in Section 4, together with the entity-specific work that will be undertaken in connection with those firms that are subject to close and continuous supervision. The supervisory strategy, its focus and planned activities reflect the particular circumstances of each sector or firm.

Back to "Contents"

Figure 3: Our supervisory priorities



Priority 1: Maintaining and building resilience to geopolitical risks and macro-financial uncertainties.

Operational and cyber resilience: Deep-dives, targeted reviews and broader thematic assessments are planned to evaluate operational and cyber resilience, including security-related risks, covering the most important sectors and firms. This includes the assessment of how firms manage the risks associated with the growing use of third party information and communications technology providers, cyber security effectiveness and the implementation of DORA requirements. In addition, there is an increasing focus on enhancing the preparedness of the system as a whole to potential operational disruptions.

Financial resilience: Given the highly volatile geopolitical and macro-financial environment, there will be ongoing monitoring of credit, market, liquidity, reserving/provisioning and business model risks along with associated risk management practices (including risk transfer) across relevant sectors. There will also be a focus on addressing data-related shortcomings evident across some sectors and firms. Work on understanding and addressing risks associated with the growing scale and increased participation in financial markets of non-bank financial institutions will continue. This includes their interaction with the banking and other sectors, including in relation to private credit.

Climate change: We will continue to scrutinise how firms are embedding climate and other environmental factors into their risk management, business models and governance. This includes assessing their responses to the increasing frequency and severity of climate related weather events - including impacts on risk appetite, credit and market risk, underwriting and pricing, provisioning/capital and liquidity - and firms' exposure to climate related litigation risk. We will

Back to "Contents"

be clear and consistent in our external communications to reinforce climate change as a priority for us given heightened macro-financial risks and, we expect, a priority for industry.

Priority 2: Securing consumer and investor interests in a rapidly changing world.

Treatment of customers: The revised Consumer Protection Code comes into effect in March 2026. Implementing the Code needs to be a priority item for firms, and supervisory work will include cross-sectoral thematic reviews focused on customer service, complaints handling and the addressing of the root causes of deficiencies, conflicts of interest, client disclosures (including the risk of misrepresentation through greenwashing) and product governance.

Digitalisation: We will continue to focus on how firms are supporting their customers as financial services continues to digitalise. We will also play our part in ensuring digitalisation does not outpace the needs of society including our work related to access to cash. We will publish regulations outlining ATM service standards relating to the hours of availability, cash withdrawal limits, and other requirements, alongside fulfilling our new licencing and oversight responsibilities under the Access to Cash legislation.[16]

Financial crime: Protecting the integrity of the financial system and consumers from financial crime needs to be a priority for all firms and agencies. We will raise awareness of fraud and scams, use our Trusted Flagger status to require the removal of criminal content online, and detect and sanction unauthorised providers and market abuse. We will assess fraud controls in banking and payments and firms' incident responses and treatment of customers.

We will focus on emerging risks and themes in anti-money laundering and controlling the financing of terrorists (AML/CFT) and how firms are ensuring their risk management frameworks keep pace with the changing nature of financial services. We will prepare for the implementation of the AML Single Rule Book and work with the Department of Finance and State agencies to strengthen the domestic framework. We will also be prioritising supporting the development of the new European AML framework working with the European Anti-Money Laundering Authority (AMLA).

[16] *Finance (Provision of Access to Cash Infrastructure) Act 2025*.

Back to "Contents"

Spotlight 3: Supporting better outcomes for consumers and investors provides more information on our approach to consumer and investor protection.

Priority 3: Responding to technology-driven transformations.

Artificial intelligence: We will continue to develop our understanding and assessment of the expanding use of AI across the value chain (including agentic AI and multi-agent systems) and reinforcing our governance and model management expections. We will also support the national implementation of those aspects of the EU AI Act that fall within our remit.

Digital money and tokenisation: Our planned activities range from our gatekeeping role in the authorisation of Crypto Asset Service Providers under MiCAR and their ongoing supervision to our consideration of how the fundamental changes to the way financial products and services are structured and delivered – including asset tokenisation, the development of stablecoins, tokenised bank deposits and a digital euro - affect consumers and established firms.

This will include a focus on the business model implications of these changes and how firms are preparing to realise the benefits of the innovations, while managing the risks. The Innovation Hub and Sandbox and the implementation of the Consumer Protection Code's requirements for digital financial services will all play a role in supporting safe innovation.

Priority 4: Helping to address the environmental and societal transitions underway.

Collaboration and research: We will continue to work in partnership with our stakeholders to help address the big challenges facing society, exploiting our data and research capabilities and our position as a well-placed convener of relevant stakeholders and experts. Over 2026/27, focus areas include flood risk, insurance protection gaps (including as one of the responsible bodies under the Government's new Action Plan for Insurance Reform 2025-2029) and low retail investment participation as part of wider EU and domestic work in this area. International engagement on sustainable finance policy will also feature as will the evolving payments landscape where we can bring

Back to "Contents"

our insights from the Innovation in Payments Sandbox Programme and International Payments Data Hackathon.[17]

Priority 5: Enhancing how we regulate and supervise.

Efficiency and effectiveness: The year ahead will see the further embedding of our revised supervisory approach introduced last year and the centralisation of our gatekeeping activities into a new division, with a specific focus on operational efficiencies and streamlining governance. We will also publish an updated version of the *Our Approach to Supervision* publication to support the better understanding of our approach by stakeholders.[18]

The Central Bank is committed to simplification and we set out our approach in our recent *Regulating and Supervising Well* publication.[19] The document includes a multi-year roadmap with key milestones for our domestic programme of work for the period 2026-2028.

Weaved throughout our work will be a continuing focus on the effectiveness of the governance and risk management practices of firms and the culture and "tone from the top" on display. This includes assessing how firms have implemented the Individual Accountability Framework (IAF) including the Senior Executive Accountibility Regime (SEAR). We will continue to use our regulatory and supervisory powers proportionately, escalated as required, to achieve our desired outcomes. We will also actively contribute to the evolution of the regulatory framework at both a domestic and EU level and the development of international standards and cooperation at global level.

[17] See Central Bank of Ireland, *Innovation Sandbox Programme – Innovation in Payments*.
[18] See Central Bank of Ireland (February 2025), *Our Approach to Supervision*.
[19] See Central Bank of Ireland (December 2025), *Regulating & Supervising well – a more effective and efficient framework*.

Back to "Contents"

Spotlight 3 – Supporting Better Outcomes for Consumers and Investors

KEY TAKEAWAYS

- The landscape consumers and investors face is volatile and complex, increasing the importance of the consumer protection framework and our work ensuring the financial system is operating in the best interests of consumers and the wider economy.
- Delivering this relies on a well-regulated and well-functioning financial sector comprised of resilient, well-run firms pursuing consumer-centric strategies.
- Our supervisory approach means that each aspect of our work – whether related to operational resilience, governance, risk management or digital transformation – is assessed with consumers' and investors' interests explicitly in mind.
- In line with our supervisory priority to *secure consumer and investor interests in a rapidly changing world*, we are focused on three high level outcomes-focused themes:
    - How firms operate and the customer experience
    - Digitalisation
    - Financial crime
- We proactively foster domestic and international collaboration with other bodies and stakeholders to deliver our mandate in an increasingly interconnected, digitalised and internationalised market for consumer and investor services.

Introduction

Ensuring the financial system operates in the best interests of consumers, investors and the wider economy is at heart of the Central Bank's work. This relies on having a financial sector comprised of resilient and well-run firms pursuing consumer-centric strategies. A key factor in shaping the work programme described in this publication has been to consider how our activities will deliver

Back to "Contents"

positive outcomes for consumers and investors in relation to the important issues affecting their lives.

We continually consider what short- and longer-term issues are being faced by listening to what consumers themselves are saying using surveys, research and direct dialogue. We join this with our own assessment of trends and risks while taking into account international consumer protection developments.[20] Our approach has also been informed by recommendations arising from a recent independent assessment by the OECD of the Central Bank against the global standards for financial consumer protection.[21] Our Consumer Advisory Group continues to play an important role in advising the Central Bank on the performance of our functions and the exercise of our powers in relation to consumers of financial services.[22]

Tackling the key issues affecting users of financial services today

The specific bodies of work planned for the coming period can be summarised under three priority headings:

- **How firms operate and the consumer experience, ensuring firms secure consumers' interests and that consumers' best interests are at the heart of decision making, systems and structures.** This includes, for example, work to improve how firms deal with customer complaints, insurance claims handling and supporting consumers in vulnerable circumstances.

- **Digitalisation, balancing the benefits of innovation with cybersecurity risks and the risk of harm to consumers.** This includes, for example, reviewing banking apps and operational resilience of digital services. Recognising the importance of availability and choice for consumers in relation to payments,

[20] The international dimension is important because, while there may be country specific contexts, risks and poor industry practices in financial services tend to feature in other jurisdictions over time. This is particularly the case when many financial services are provided in multiple countries by very large global organisations.
[21] See Central Bank of Ireland (December 2024), *OECD publishes outcome of review of Central Bank's consumer protection supervisory functions, Central Bank of Ireland*.
[22] See *Consumer Advisory Group*, Central Bank of Ireland.

Back to "Contents"

we will also implement the provisions of the Access to Cash legislation.[23]

- **Financial crime, safeguarding the integrity of the financial system and consumer interests by combatting fraud, scams and other financial crime including market abuse and money laundering.** This includes, for example, continuing engagement with social media platforms and other technology providers and working with and through other public bodies with parallel or adjacent functions. We will also require the firms we regulate to enhance their safeguards against fraud and put better supports in place for consumers and investors who fall victim to fraud.

A key element running through our supervisory efforts is the implementation of the revised Consumer Protection Code, effective from March 2026. The Code continues to be the cornerstone of Ireland's consumer protection framework. The changes coming into force in March have been designed following extensive public consultation to ensure the Code better reflects the way financial services are provided today and enhances clarity and predictability for firms on their consumer protection obligations.

Our expectations of firms are encapsulated in the Code and will be to the forefront of our day-to-day and thematic supervisory engagements with firms, making the revised Code a "living regime" rather than merely a compliance check list. The new supervisory approach we introduced last year means that each aspect of our work – whether related to operational resilience, governance, risk management or digital transformation – is assessed with consumers' and investors' interests explicitly in mind.

We have highlighted the drivers of conduct risk in several of our publications and discussions with the financial sector over recent years and these remain a focus for supervisors. Experience tells us that problems arise – and recur in too many instances – when there are poor business practices and weak business processes, ineffective disclosures to consumers and investors, inadequacies in culture, governance and risk management, and ineffective management of conflicts of interest. These factors are compounded by the rapidly changing operational and technological landscape or if firms make

[23] *Finance (Provision of Access to Cash Infrastructure) Act 2025*. This includes fulfilling new responsibilities under the legislation, such as monitoring compliance with the access to cash criteria and the oversight of ATM operators and cash-in-transit providers.

Back to "Contents"

business model or strategy changes without having proper regard to their impact on their customers. Evidence of these drivers continues to be seen across sectors and firms and must be properly tackled if customer-centric cultures and processes are to be truly embedded.

Sections 3 and 4 provide further insights into our supervisory priorities and planned activities for securing consumer and investor interests as they relate to different sectors, products and services.

Working with other stakeholders for better consumer outcomes

Given the more interconnected, cross border and digitalised nature of financial services, increasingly many of the financial challenges the public face will only be solved by stakeholders across the domestic and international community working together. We will continue to play our part in identifying and supporting collaborative solutions to these challenges. In 2026 key areas of focus for us will be to support the Government's National Financial Literacy Strategy and the Action Plan for Insurance Reform. Through our Consumer Hub and digital channels, we will also continue to provide information to consumers and investors to inform them of the potential risks they face, the benefits of participation in the financial system and the requirements placed on firms to support their consumer experience.

A key role we will continue to play is to bring empirical evidence to the table on consumers' experiences and the risks they face against the rapidly changing backdrop. By doing so publicly and systematically we also equip consumer advocates and civil society with information they may not otherwise be able to gather or analyse. Recently this has included research into buy now pay later (BNPL), high-cost credit and retail investor participation.

We will continue to monitor the effectiveness of our consumer and investor protection frameworks to ensure they remain fit for purpose in the rapidly changing financial system which includes more providers operating in Ireland from bases in other countries. In 2026 we will continue our active involvement in international bodies, with a focus on work at the OECD, IOSCO, and FinCoNet[24] and supporting supervisory convergence and common standards in the European Supervisory Authorities' (ESA) consumer protection

[24] FinCoNet is an international organisation of supervisory authorities which have responsibility for market conduct and financial consumer protection.

Back to "Contents"

work. The ESA programme complements national supervisory mandates and contributes to the harmonisation of conduct supervision across the EU.

Conclusion

Consumer and investor protection is at the heart of the Central Bank's mandate. Under our new supervisory framework, we deliver on this mandate through an extensive work programme which:

- Tackles the key issues affecting consumers as evidenced by consumer complaints, research and international analysis
- Continues to build our consumer and investor protection framework for the future, and
- Fosters domestic and international relationships and supports the initiatives we need to deliver our mandate in an increasingly interconnected, digitalised and internationalised market for consumer and investor services.

Back to "Contents"

Section 4 – A Sectoral Focus

Introduction

In this section, trends, risks and vulnerabilities are considered from a sectoral perspective in line with our supervisory approach. The cross-cutting risk themes outlined in Section 2 will have varying degrees of relevance for each sector. As a result, the Central Bank's sectoral supervisory strategy and key activities for the period ahead reflect the profile and risk outlook of the sector they cover.

We will be undertaking a range of cross-sectoral, sectoral and firm-specific supervisory work covering the spectrum of risk areas. This includes direct engagement with firms and deep dive inspections, thematic reviews and data analysis. Where material breaches of regulations are identified and supervisory concerns persist despite regulatory engagement with firms, the Central Bank has recourse to a range of escalation tools, including enforcement.

Approach

For each sector, we provide a sectoral assessment and the key areas of supervisory focus. The key risks identified are informed by the Central Bank's market monitoring, horizon scanning and sectoral risk assessments, as well as the risk assessment work undertaken by ECB Banking Supervision and the European Supervisory Authorities and engagement with other stakeholders such as the Consumer

The main supervisory activities we have planned in relation to each focus area with indicative timelines are set out. The aim is to provide firms with greater visibility of our work plans. In some instances where key pieces of work will continue into 2027, this has been shown.

It is important to note that the lists of activities listed are not exhaustive and sit alongside ongoing supervisory work and engagement and may be subject to change should circumstances change or events arise that require reprioritisation.

Back to "Contents"

Banking & Payments

Back to “Contents”

Banking Sector

KEY TAKEAWAYS

- Banking is evolving rapidly driven by digitalisation and increased competition. Incumbent banks face many strategic challenges from fintech and non-bank competitors, new types of money and changing consumer expectations, while the challenge for newer players is to build an operational capability that is commensurate with their growth ambitions. Effective board oversight and change management is critical.
- The sector has shown financial resilience in the face of overlapping global shocks and periods of significant financial volatility, with continued profitability. This is in part due to unprecedented fiscal and monetary policy interventions that may not be repeatable. Market valuations have improved, yet normalising funding costs and the potential for higher impairments mean banks should avoid complacency.
- The volatile operating environment and the increasingly evident impact of climate change means that banks need to continue to deepen their understanding of their asset and liability risk exposures over different time horizons, including physical and transition risks, supported by improved data, modelling and scenario analysis.
- Banks must continue building trust and be able to demonstrate how they are securing their customers' interest and embedding their obligations under the Individual Accountability Framework, Consumer Protection Code and DORA.
- This sectoral assessment complements the Central Bank's risk based supervisory approach as part of the ECB's Single Supervisory Mechanism (SSM) and sets out 2026 priorities to safeguard financial stability, resilience and secure customers' interests.

Sector profile

- Globally oriented sector, with approximately 60% of industry assets held by internationally facing banks.
- Internationally facing banks provide a diverse range of products and services to a global client base. Assets of c.€456bn at Q4 2025 (up 3% on end 2024). Continued growth in this segment of the sector is expected in 2026.
- Domestic retail banks serve Irish households and businesses, with some significant exposures also to the UK market. Assets of c.€317bn at Q4 2025 (up 3% on end 2024).

Back to "Contents"

- Several banks operate in Ireland from other EEA jurisdictions offering savings, loans and payment services.

Our supervisory approach to the sector

Our strategy for the sector prioritises those risks and vulnerabilities that we believe pose the greatest threat to the delivery of the Central Bank's safeguarding outcomes, with supervisory activities conducted as part of the SSM.[25] Alongside on-going direct engagement with firms, planned activities include data analysis and monitoring of early warning indicators, firm specific deep dives and on-site inspections, SSM led thematic reviews, a planned SSM reverse stress test and thematic reviews across a range of risk areas with a particular focus on fraud, conduct and AML/CFT risk.

We are actively engaged in simplification discussions at an international level with the ECB/SSM (and with SRB/SRM) and other EU supervisory authorities. In parallel, domestic frameworks are under review to simplify requirements where appropriate and streamline processes while preserving resilience, stability and consumer protections. In a banking context, progress has been made through the implementation of our integrated supervisory framework and in rationalising some reporting requirements for the sector. The SSM is also advanced in streamlining certain supervisory processes through its "Next Level Supervision" initiative.[26]

Sectoral assessment and supervisory focus areas

Focus Area 1: Business model and strategy

The domestic and international banking sector is evolving and growing strongly because of new entrants, the expansion of business activities and the arrival of cross-border providers from other EEA member states.[27] New entrants, which generally operate through digital channels rather than a branch network, bring greater choice and often act as a catalyst for market innovation. Offerings include current accounts, payment services, deposits, shorter term lending - including "buy now pay later (BNPL)" loans - and mortgages.

[25] See European Central Bank (November 2025), *Supervisory Priorities 2026-2028*.
[26] See European Central Bank (December 2025), *Streamlining supervision, safeguarding resilience*.
[27] Banks licenced in one member state may, subject to notification, provide services on a freedom of service (cross border) or freedom of establishment (branch) basis in other member states.

Back to "Contents"

It is important that the strategies and plans of new entrants and incumbents have the interests of customers as a focal point and that firms have the financial and operational resources to deliver them safely.

Article 21c of the Capital Requirements Directive (CRD6) comes into effect in January 2027 requiring undertakings established in a third country such as the UK to establish an EU subsidiary or a series of local third country branches to carrying out the in-scope banking activities within the EU. This will result in new entrants to the Irish banking sector and material business transformations for some existing operations. Any transfer of assets and liabilities to Irish entities can materially change risk profiles and affected firms need to enhance their risk management and control frameworks accordingly to cater for new business lines and new markets.

In parallel, the rapidly evolving payments ecosystem is bringing benefits for consumers and banks but also challenges. Banks can better support their customers and the broader economy by providing instantaneous transactions 24/7, both domestically and on a global cross border basis, but this must be done in a safe and secure manner. As incumbent players adapt and transform legacy IT platforms, and new entrants seek to grow, each must ensure that their change management, governance and financial arrangements keep pace with the complexity of their operations and the risks they take on.

Both established and new providers should prioritise consumer interests throughout any changes to existing products and services, the introduction of new ones, and in how these are delivered and serviced. Consumers, particularly those in vulnerable circumstances, could be exposed to financial harm as the delivery of banking products and services moves away from traditional channels.

The main planned activities relating to this supervisory focus area are:

Back to “Contents”

		H1 26	H2 26
1.1	Reviews of banks' **corporate strategy setting**, alignment with risk appetite and the credibility of the underlying assumptions.	●	●
1.2	Assessments of **banks' strategies given the evolution in payments**, the National Payments Strategy, access to cash requirements, roll-out of P2P payments (e.g. Zippay), digital euro, stablecoins and tokenisation. with a targeted engagement depending on the nature, scale and complexity of any impacts.	●	●
1.3	Assessment of the **impact of CRD6 Article 21c** on banks' balance sheets. Supervisors will undertake tailored engagements with impacted banks depending on the nature, scale and complexity of any impact.	●	●
1.4	Assessment of **new bank licence applications** in collaboration with the ECB as part of the SSM.	●	●
1.5	Assessment of bank-specific **growth strategies and/or new business lines** to understand growth ambitions and if they appropriately consider consumer and investor interests and are underpinned by effective governance and risk management arrangements, and operational and financial capacity.	●	●

Focus Area 2: Treatment of customers

In the course of our supervisory work, we continue to see instances where actual harm or the heightened risk of harm arises because customers' interests are not being fully embedded in board-level and day-to-day decision making. This can manifest itself in poor customer service and errors, unclear customer information, or the failure to properly identify customers in vulnerable circumstances and treat them appropriately. Poor governance and oversight are often a root cause of these issues and banks need to prioritise reviewing and ensuring products are suitable for their customers and proactively engaging with borrowers in or facing arrears.

During times of business and operational change, for example, moving from in-person to digital or remote service provision, strong governance and appropriate oversight are essential. The obligations banks have under the updated Consumer Protection Code, Access to Cash regime and IAF, if properly embedded, are

Back to "Contents"

designed to help mitigate these risks, but ultimately it is the culture within the bank that is the key mitigant.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27
2.1	Cross-sectoral review of how banks are carrying out **root cause analysis of errors** and applying learnings to their wider product and service suite.	●	●	
2.2	Thematic review of the **sale of products via banking apps** with a focus on how banks identify and mitigate risk to consumers on a sample of products sold.	●	●	
2.3	Cross-sectoral thematic review of **customer service standards** including, in the banking and lending sector, a review of the impact on customer service of supervisory actions arising from previous conduct-related thematic reviews.	●	●	
2.4	Cross-sectoral thematic reviews on: – **how customers are being informed** effectively and – treatment of **customers in vulnerable circumstances.**	●	● ●	 ●
2.5	Review of how banks are securing customers' interests in the **operation of current accounts**.	●	●	
2.6	Enhancing our data to support retail conduct supervision, including **enhancing the conduct of business return** and data on areas of elevated risk such as fraud.	●	●	
2.7	Cross-sectoral thematic review of **BNPL arrangements**.	●	●	
2.8	Cross-sectoral thematic review of **mortgage lending** to include an analysis of credit, loan origination and risks to borrowers (including monitoring for early signs of **over-indebtedness or distress**).		●	●

Focus Area 3: Operational and cyber resilience

Banks' growing use of technology to deliver services and to improve efficiency, together with the sector's pivotal role in the

Back to "Contents"

economy, increase their risk exposure to operational outages and malicious cyber-attacks. The probability of such events has increased in the current geopolitical environment. The risk of disruption is heightened by growing dependencies on third-party service providers, including for critical specialist services such as cloud computing, telecoms, data centres and AI. We have seen, for example, a rise in cyber threat levels via reported bank-related distributed denial of services (DDoS) attacks compared to 2024.[28] While the introduction of DORA strengthens the regulatory framework, its effectiveness depends on being properly implemented.

So far, the impact of such DDoS events and other disruptions has been limited in duration but this may not always be the case. The mitigation of operational and cyber risk requires banks to properly control what they can control and be able to respond and recover promptly when something outside their control happens. This requires banks to have effective ICT and operational risk management frameworks and executable contingency plans in place. These must cover both their own operations and those for which they remain responsible that are delivered by their outsourced service providers (including those on which their key outsourced service providers rely).

The sector's growing dependence on digital channels to deliver services to customers is placing increasing demands on banks' capacity to manage significant and complex IT change programmes. Banks need to have the capability to manage change effectively and, when things go wrong, they must be able to address the root cause. They must also consider the impact on their customers, be timely and clear in their communications and remediate promptly and appropriately.

The main planned activities relating to this supervisory focus area are:

[28] DDoS is a type of cyber-attack where multiple compromised systems flood a target (e.g., a bank's website or apps) with traffic or requests, overwhelming it so legitimate users cannot access services. For financial institutions, DDoS can disrupt online banking, payments and market data services, and may be used to distract from other malicious activity.

Back to "Contents"

		H1 26	H2 26
3.1	Key focus areas for significant institutions include: – Targeted follow-up on **remediation strategies** for those banks that report material shortcomings in **ICT security/cyber-security resilience** and **ICT outsourcing**. – On site inspection campaigns on **cyber security management** and **third-party risk management**, in line with the new **DORA** requirements. – **Threat-led penetration testing** to identify banks' vulnerabilities and improve their cybersecurity resilience. – Targeted review of **ICT change management**. – Deep dive into banks' dependency on **cloud service providers** to assess their preparedness for potential service disruptions.	●	●
3.2	Firm specific follow up from the **2025 thematic review on operational resilience** for international LSIs.	●	●
3.3	Supervisory assessment of **cyber resilience remediation programmes**.	●	●
3.4	Tracking **remediation of outsourcing deficiencies** identified in previous reviews.	●	●
3.5	Continued engagement with banks and interventions where **outages** occur, including focus on communications, customer service and customers in vulnerable circumstances.	●	●
3.6	Continued work with industry and government to establish a collective action approach to **system-wide operational resilience** for payment services (including cash).	●	●

Focus Area 4: Financial resilience

The banking sector has demonstrated financial resilience against a challenging economic backdrop and increased competition from the non-banking sector and specialist providers. Irish banks participating in the 2025 EBA stress test performed strongly, with capital buffers under adverse conditions remaining well above

Back to "Contents"

minimum requirements.[29] Domestic banks' profitability is supported by interest income, increased income diversification and a deposit base that is currently very stable. Asset quality has, on aggregate, been maintained. International banks' profitability has benefited from an environment that is supportive of their primarily cross-border wholesale activities such as corporate and investment lending, markets and treasury trading, structured finance and securitisation.

Sustained financial resilience requires banks to ensure that their capital and liquidity management is aligned to their risk exposures, appropriately calibrated and sufficiently risk sensitive. Banks need to adopt prudent risk-taking and sound underwriting standards recognising the uncertainties of the external environment. This requires a forward-looking perspective with the use of scenario analysis to consider in a structured way the implications of different possible futures. Complacency about the future, of which we see some evidence in some banks, needs to be avoided.

The effects of climate change are affecting banks and their customers through their impact on credit lines or the value of real assets exposed to physical and transition risks in Ireland and overseas. Examples include buildings located in widening flood zones or which do not meet the environmental standards expected today. While crystallised physical risks, such as the damage wrought by natural catastrophes, are more visible, the second-round effects - such as disruptions to supply chains, reduced economic activity, input price increases, or increased credit defaults - are less well understood. Some banks have made material progress on embedding the assessment and the management of short, medium and long-term risks stemming from the climate and nature crises into their risk management frameworks in a way that is commensurate with the risks they face, but others need to keep building on progress to date.

Sound financial management can be undermined if deficient data management and reporting capabilities hamper a bank's ability to monitor and manage risks across the business. The weaknesses we see in some banks' RDARR[30] frameworks can impede a holistic view of individual and total risk exposures. This can in turn undermine strategic decision making and impair the regulatory and risk reporting upon which we rely. As the use of more sophisticated

[29] See EBA (August 2025), *The EBA publishes the results of its 2025 EU-wide stress test*.
[30] Risk Data Aggregation and Reporting Requirements (RDARR)

Back to "Contents"

models to support decision making increases and AI capabilities are deployed – for example in connection with lending and trading strategies – any deficiencies in a bank's model risk management and oversight practices need to be addressed.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26
4.1	**SREP risk assessments** (incorporating CRR3/CRD6 climate and nature aspects), including for significant institutions the implementation of the **new P2R methodology**.[31]	●	●
4.2	Supervisory assessment, qualitative and quantitative analysis of **credit** (including climate and nature aspects), **loan origination**, **vulnerable sectors**, **short-term lending e.g. BNPL**, mortgage lending, and **risks to borrowers** including customer indebtedness. Follow up on issued credit risk management **Risk Mitigation Programmes** (RMPs).	●	●
4.3	Assessment of Pillar 1 capital requirements for SA under CRR3 in **credit risk and market risk**, along with planned **internal model investigation** work responding to banks' submission of updated/new IRB models.	●	●
4.4	**Financial resilience assessments**, incorporating capital position assessments, distribution strategies, securitisation, provisioning (IFRS9), liquidity, market risk and recovery planning.	●	●
4.5	Identification and assessment by the Central Bank of **transmission channels**, **cross-cutting risks** and **cross-sectoral interlinkages** arising from macroeconomic and geopolitical risks (including geopolitical reverse stress test coordinated by the SSM).	●	●
4.6	Reviews of the **remediation of shortcomings** in the integration of **climate and environmental risks** into banks' risk management frameworks, in addition to consideration of ESG transition plans.	●	●
4.7	**Remediation of RDARR deficiencies** identified from reviews in previous years.	●	●
4.8	**Assessment of the AI landscape in the banking sector** to build supervisory knowledge on AI use and support the Central Bank's	●	●

[31] See European Central Bank (November 2025), *Supervisory Priorities 2026-2028*.

Back to "Contents"

		H1 26	H2 26
	work in developing its supervisory approach on AI applications and the EU AI Act. Support SSM work to strengthen supervisory understanding of how banks use generative AI applications.		

Focus Area 5: Financial crime and market integrity

The banking sector by its nature is inherently high risk from a money laundering, terrorist financing and fraud perspective. Not only are banks the main gateway to access the financial system for households, businesses and consumers, but also for criminals. Thanks to efforts over the past decade, traditional banks' AML/CFT frameworks are generally mature and well embedded. As the banking sector diversifies in Ireland, there is a need for newer entrants to continue to build and strengthen their AML/CFT frameworks, in line with national and European requirements, including those of AMLA. Boards and senior management must be able to demonstrate an understanding of their bank's key ML and TF risks and the adequacy of their risk management and control frameworks.

Consumers and banks are increasingly being targeted by new and sophisticated ways to launder the proceeds of crime. Given the important role banks play in combatting "dirty money" entering the financial system, they need to be particularly vigilant and responsive to criminals exploiting new technologies and practices to abuse the system, and firms within it. While developments in digitally enhanced business models provide many benefits for consumers and enhance the ease and speed of access to financial services, there is a corresponding increase in the risk of exploitation by criminals to launder the proceeds of crime or perpetrate scams and fraud, as well as increased risks of mis-selling and misrepresentation.

The nature of fraud is evolving rapidly. International fraud networks are becoming more sophisticated, taking advantage of social media platforms and increasingly using AI tools to evade bank controls and exploit customers, including those in vulnerable circumstances. Banks must do more to strengthen their controls, including improving data and management information, and enhancing transaction monitoring and IT security systems to reduce the likelihood of frauds and scams occurring. Where fraud does occur, banks need to provide appropriate and timely support to affected customers.

Back to "Contents"

Wholesale financial markets and risks to market integrity continue to evolve with increased electronification and the application of AI to business models. These changes are driving structural changes and technological innovation in wholesale banks, and this places greater demand on bank's frameworks for the management of market conduct risk. In the course of our supervisory work and market oversight we continue to observe deficiencies in banks' frameworks for the monitoring and mitigation of market conduct risk. A root cause continues to be the failure of banks to comprehensively identify all market conduct risks emanating from their business activities. This can manifest in conflicts of interest not being appropriately identified and mitigated, surveillance frameworks for the detection of potential market abuse not keeping pace with business activities, and deficiencies in first line of control frameworks.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27
5.1	Assessment of individual banks and aggregated sectoral data from the **enhanced AML/CFT Risk Evaluation Questionnaire (REQ) submissions**. The enhanced REQ will capture detailed quantitative and qualitative risk information on ML/TF risk and the quality of AML/CFT controls. This data will be used to: (a) identify firm and sector-specific issues and emerging trends; (b) conduct desk-based supervisory reviews of firms and guide supervisory strategy; and (c) input into the development of a new EU AML Risk Assessment Methodology (led by AMLA). *Data submission in H1 with assessment during H2.*	●	●	
5.2	**Targeted supervisory engagements**, including inspections, desk-based reviews and review meetings.	●	●	
5.3	Cross-sectoral thematic review of **controls** on certain types of **fraud** as well as the **fair treatment of customers** who fall victim to fraud.	●	●	
5.4	Cross-sectoral thematic review of **conflicts of interest** management in **wholesale market banks**.	●	●	

Back to "Contents"

		H1 26	H2 26	H1 27
5.5	Cross-sectoral thematic review of **market abuse frameworks** and **surveillance**.	●	●	
5.6	Cross-sectoral thematic review of **unauthorised trading** and **trading controls**.		●	●

Back to “Contents”

Payment and E-Money Sector

KEY TAKEAWAYS

- Business models are evolving, with more firms seeking multiple licences, particularly relating to crypto-asset service provision and the issuing of electronic money tokens (EMTs).
- Achieving sustainable profitability is proving challenging for some. Any consequent consolidation, exit or failure must be managed in an orderly way with customers' interests at the heart of decision-making.
- While progress is being made on addressing deficiencies the Central Bank has highlighted in the past, there continue to be areas requiring improvement, in particular, ensuring customers' interests are properly considered in decision-making. A lack of such consideration is often the root cause of problems such as the weak safeguarding of customers' funds and poor customer experiences.
- The sector is at high risk of being used as a vehicle for financial crime given the large volume of transactions, international reach and diverse and complex nature of business models. We continue to identify weaknesses in firms' understanding of their money laundering and terrorist financing risk exposures leading to ineffective risk frameworks.
- We will be engaging with e-money firms on the European Commission's clarification of the definition of electronic money and its impact on the sector and their activities.

Sector profile

- Payment and e-money firms have an increasingly important role in the European payments system architecture and are key players at the forefront of the digital transformation of the financial services sector.
- 58 authorised firms with safeguarded funds of €11.8bn at end 2025 (up 17% on end 2024) and payment transactions of €702bn in 2025 (up 14% on 2024).
- Firms range from small start-ups entering the regulatory perimeter for the first time to more established non-bank international groups, or bank subsidiaries, which offer payment services across the EEA.

Back to "Contents"

- Sector has a diverse range of business models providing services including merchant acquiring, money remittance and e-money issuance, which facilitate consumers making and merchants accepting payments in electronic form.

Our supervisory approach to the sector

Our supervisory activities and interventions are undertaken on a sectoral basis, with firm specific engagement where appropriate. Planned activities are set out below and cover five focus areas. They include thematic reviews across a wide range of risk areas with a particular focus on safeguarding, governance structures, consumer protection and AML/CFT risk.

Sectoral assessment and supervisory focus areas

Focus Area 1: Safeguarding of customers' funds

Protection of customer monies remains one of the most important objectives for the Central Bank and firms are reminded that we have no tolerance for weaknesses in safeguarding arrangements. As customer funds held by firms in this sector are not protected by a deposit guarantee scheme, unlike deposits held by Irish banks and credit unions, it is vital that firms have effective and appropriate safeguarding frameworks to ensure that customers' funds are protected on an ongoing basis. Reflecting the importance of safeguarding, we have extended our Pre-Approved Control Function (PCF) regime to include a new PCF Head of Safeguarding, effective from February 2026.

We have undertaken extensive work on safeguarding in recent years, including inspections and third-party audits of all firms' safeguarding processes, with our findings and expectations clearly communicated. A thematic inspection assessing the operational effectiveness of firms' safeguarding processes and control infrastructure was completed last year. While the inspection identified some good practices, significant deficiencies continue to be identified despite the supervisory work previously undertaken and the feedback provided. These were set out in the recent Payment and E-Money Newsletter.[32]

We expect all firms to keep their safeguarding frameworks and processes under constant review, including consideration of all

[32] See Central Bank of Ireland (December 2025), *Payment and E-Money Newsletter*.

Back to "Contents"

findings and supervisory expectations communicated, irrespective of whether an individual firm was directly included in the work. Where firms identify gaps or weaknesses in their frameworks or processes, they should take appropriate and timely remediation actions to ensure that customer funds are always protected.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26
1.1	Assessment of the actions taken by firms to **address identified gaps in safeguarding** processes and procedures.	●	●
1.2	Assessment of firms' implementation of the new **Head of Safeguarding PCF role**.	●	●

Focus Area 2: Financial crime

The payment and e-money sector has inherently high exposure to the risk of financial crime, including money laundering, terrorist financing and fraud. The reason for this is that the business models in this sector are diverse and complex, typically handling a high volume of transactions with a wide international reach.

The use of technology and innovative ways to serve the needs of consumers is welcome for reasons of both efficiency and convenience. However, this exposes firms to heightened risks that they, and their customers, will be abused by criminals to launder the proceeds of crime, finance terrorism and perpetrate fraud and scams. Firms need to remain vigilant and keep pace with financial crime risks and typologies associated with new technologies.

There has been an expansion of cybercrime and fraud in recent years, with AI driven social engineering becoming a primary threat, and this continues to challenge the sector's defensive capabilities. In 2024, €57m of fraudulent payments were recorded by Irish resident payment and e-money institutions representing a three-fold increase on the previous year. The value of transactions was 66% higher over the same period with the level of fraud relative to transactions increasing for both e-money transactions and money remittance.[33] We continue to receive a high level of protected

[33] Based on analysis of payment fraud statistics.

Back to "Contents"

disclosures indicating individuals transacting with the sector who have been the victim of fraud events. Firms must ensure they have robust systems for detection and prevention of fraud and are putting customer needs first, especially customers in vulnerable circumstances.

The inherent ML/TF risk facing firms is high and continues to increase given the changing nature of sector.[34] While some firms have taken positive steps to strengthen their AML/CFT risk management and control frameworks, further work is required across the sector to build and strengthen frameworks, particularly by new entrants. A key concern is firms' inadequate understanding of ML/TF risks and the need for adequate mitigating measures commensurate with the risks. Firms' governance arrangements, systems and controls, including reporting mechanisms, need to be effective and proportionate to the nature, scale and complexity of their business, and the risks to which they are exposed.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26
2.1	Assessment of the adequacy and effectiveness of **AML/CFT risk management frameworks** through AML inspections, targeted and thematic reviews and financial crime review meetings.	●	●
2.2	Assessment of individual firm and aggregated sectoral data from the **enhanced AML/CFT Risk Evaluation Questionnaire (REQ) submissions**. The enhanced REQ will capture detailed quantitative and qualitative risk information on ML/TF risk and the quality of AML/CFT controls. This data will be used to: (a) identify firm and sector-specific issues and emerging trends; (b) guide supervisory strategy; and (c) satisfy incoming data requirements for the EU's Anti-Money Laundering Authority (AMLA).	●	●
2.3	Cross-sectoral thematic review of **controls** on certain types of **fraud** as well as the **fair treatment of customers** who fall victim to fraud.	●	●

[34] See EBA (July 2025), *Opinion on money laundering and terrorist financial risks affecting the EU's financial sector*.

Back to "Contents"

Focus Area 3: Business models and financial resilience

Recent years have seen significant growth in the sector across Europe resulting in intensifying competition. Additionally, we continue to receive a high level of material change in business models requests and acquiring transaction notifications. This reflects the number of firms adapting their business models to respond to increased competition. Firms are focusing on competitive differentiation through innovation. However, high operating costs and limited sustainable funding options make some firms financially vulnerable. The financial risks facing the sector are exacerbated by the uncertain macroeconomic and geopolitical environment and a potentially saturated market.

Financial resilience challenges are likely to lead to sectoral consolidation, or the exit or failure of certain firms, reinforcing the need for bespoke, effective and actionable wind-down plans. In our supervisory work we have observed that wind-down plans are not consistently aligned to a firm's risk management framework and have inadequate triggers to ensure, where required, an orderly and solvent wind-down. Firms are not adequately considering potential obstacles to executing a wind-down, particularly relating to the timely and full return of customer money. We expect firms to have credible plans which, inter alia, prioritise the return of customer money in an efficient and timely manner in the event of an exit or wind-down situation. In support of orderly firm failure, the National Payment Strategy outlined that the Department of Finance, following input from the Central Bank, will examine the need to provide the Central Bank with liquidation powers in relation to payment firms.[35]

The European Commission has clarified the conditions under which e-money exists.[36] This clarification has a direct impact on the products and business models of some e-money institutions (EMIs). We will continue to engage with firms on the impacts of this issue, including on the regulatory impacts and the timelines for implementation of any necessary changes**.** In advance of this engagement, EMIs should assess what implications the Q&A may have for their business model or products, if any, and what potential actions they will need to take to comply. Firms seeking authorisation as an EMI should also assess the implications of the Q&A for the

[35] Department of Finance (October 2024), *National Payment Strategy*.
[36] See the response to the question with ID 2022_6336 relating to the definition of electronic money in *Q&A 2022_6336*, EBA.

Back to "Contents"

activities they are proposing to undertake within their authorisation application.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26
3.1	Thematic review of **financial resilience**, including **strategic planning** and **wind down planning**.	●	●
3.2	Engagement with firms in the sector regarding the **Q&A 2022_6336**.	●	●

Focus Area 4: Operational and cyber resilience

The movement of money through the financial system is critically dependent on operational resilience to ensure the reliability, availability, security and recoverability of the services being provided. Operational disruptions and the unavailability of important business services - which may arise due to internal or external factors including cyberattacks, IT system outages or third-party supplier failure - have the potential to cause harm to consumers, threaten the viability of firms and cause instability in the financial system. We continued to see increased levels of system outages reported as major incidents in 2025, including cross industry disruption impacting the payment system as a whole and subsequently causing customer disruption.

Firms are increasingly vulnerable to cyberattacks given the geopolitical context and the complexity of the networks of third-party outsourced service providers they rely on. Firms must prioritise robust cybersecurity measures, including data encryption, multi-factor authentication and regular penetration testing to safeguard their systems and customer data.

Outsourcing of services to third parties, including intra-group providers, remains a key risk in the sector due to instances of inappropriate or ineffective oversight. Firms need to ensure that they have appropriate governance, management and oversight of outsourcing arrangements, together with rigorous contingency and exit planning. We commenced a thematic review of the governance and effectiveness of IT outsourcing across several firms in the sector

Back to “Contents”

last year which will conclude in 2026, and we will be communicating the findings and our expectations in due course.

The main planned activities relating to this supervisory focus area are

		H1 26	H2 26
4.1	Issue feedback on the thematic review of the **governance and effectiveness of IT outsourcing**.	●	
4.2	Targeted **follow-up on remediation strategies** for those firms where issues have been identified in relation to their management of **operational and cyber risks and resilience**.	●	●
4.3	Supervisory assessment of **DORA** reporting, including Registers of Information (RoI) and major incident reporting, to inform the Central Bank's assessment of operational resilience at a sectoral and firm specific level.	●	●
4.4	Focus on the implementation and development of incoming regulations and initiatives, in particular the **Payment Services Directive (PSD3)** and **Payment Services Regulation**.	●	●
4.5	Continued work with industry and government to establish a collective action approach to **system-wide operational resilience** for payment services (including cash).	●	●

Focus Area 5: Culture, governance and risk management

Our supervisory work has regularly identified the absence of a customer-centric culture whereby customers' interests are not being consistently placed at the heart of decision making. In certain firms we have seen evidence of customer interests being neglected in the pursuit of new business growth. Firms are expected to maintain both perspectives in equilibrium, ensuring that business models and practices are centred on customers' interests while being sustainably profitable.

A 2025 thematic review examining customer experience through the lens of customer complaints highlighted that some firms are still failing to appropriately identify complaints when consumers express a grievance or dissatisfaction. This is a requirement of the Consumer Protection Code. Many firms do not address the root causes of the complaint which leads to recurring issues and

Back to "Contents"

complaints progressing unnecessarily to the Financial Services and Pensions Ombudsman.[37]

While acknowledging the scale and complexity of firms differ in the sector, appropriate leadership and oversight by boards and senior management must form the foundations of all firms. Firms, including those who operate as part of a wider group, must be able to demonstrate that they have effective governance and risk management arrangements in place to respond to the range of risks facing firms and to ensure customer interests are secured.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
5.1	Cross-sectoral thematic review of **whether customers are being informed effectively**.	●	●		
5.2	Cross-sectoral review of how firms are carrying out **root cause analysis of errors** and applying learnings to their wider product and service suite.	●	●		
5.3	Cross-sectoral thematic review of the **identification and treatment of vulnerable customers**.	●	●	●	
5.4	Assessment of **board composition**, **resourcing levels** and **governance structures**.			●	●
5.5	Thematic review of the **operation of distributors and agents model**.			●	●

[37] Central Bank of Ireland (December 2025), *Payment and E-Money Newsletter*.

Back to "Contents"

Retail Credit Sector

KEY TAKEAWAYS

- The upcoming revised Consumer Protection Code will require firms to embed consumer interests at the heart of their culture, strategy and business models.
- Firms must adopt prudent lending practices and only engage in responsible lending, which requires clear product explanations. Short-term credit arrangements pose over-indebtedness risk including consumers' misunderstanding of associated risks.
- There is a growing need for firms to consider how the evolving market impacts on their business. They must ensure that their business models are financially and operationally sustainable and that their governance, risk management and internal control frameworks keep pace with their changing risk profiles.
- Firms must be financially and operationally resilient. Their strategies should be developed and owned by the boards of the Irish entity with adequate resources deployed to support current operations and future growth ambitions, with appropriately skilled and experienced personnel.

Sector Profile

- The sector comprises 36 retail credit firms (RCF), 19 credit servicing firms (CSF) and 28 high-cost credit providers (HCCPs).
- Diversity of business models ranging from non-lending firms managing large portfolios of distressed loans sold by the domestic retail banks to non-bank financial institutions, through to lending firms offering mortgages, personal loans, asset finance such as hire purchase, cash loans, premium finance and credit for goods from online retailers.
- Total assets under management of c.€47bn at end June 2025 (versus c.€48bn as at end 2024). HCCPs had balances outstanding of c.€110m driven primarily by premium finance companies as at end 2024.
- Customer accounts amount to c.958k accounts, of which retail credit firms total c.535k, credit servicing firms c.135k and HCCPs c.288k.

Back to "Contents"

Our supervisory approach to the sector

Our supervisory activities and interventions are undertaken on a sectoral and cross-sectoral basis, with firm specific engagement where appropriate. There is a particular focus on mortgage lending, operational resilience and customer service and protection, and the introduction of a sector specific ML/TF Risk Evaluation Questionnaire (REQ).

Sectoral assessment and supervisory focus areas

Focus Area 1: Treatment of customers

Shortcomings in the treatment of customers often stem from a weak consumer-focused culture, poor governance, inadequate controls, and risk frameworks that lag business growth. Whilst firms have made improvements in securing customer interests, they must be proactive in dealing with customers and importantly in implementing and embedding the revised Consumer Protection Code coming into effect in March 2026.

Our supervisory concerns relate to how firms identify, manage and respond to customer complaints, learn from them and use those learnings to create a culture that is more customer centric. We have also observed instances where some firms were not managing interest rate pass-throughs and addressing identified errors in a timely manner. This resulted in supervisory intervention. The Code strengthens consumer protections and reinforces our expectation that firms are well-run, prioritise customer interests and effectively manage conflicts of interest.

We continue to focus on both retail credit firms' and credit servicing firms' initiatives to reduce the number of accounts in long-term mortgage arrears and the prevention of new accounts entering arrears. We expect firms to act with integrity in managing arrears and in dealing with borrowers in or facing arrears.[38] There is a need for firms to continue to proactively engage with borrowers and ensure alternative repayment arrangements implemented are appropriate and sustainable in accordance with Central Bank guidance.[39] It is the firm's responsibility to fully adhere to the

[38] See Central Bank of Ireland, *Customer Protection Code and Regulations*.
[39] See Central Bank of Ireland (January 2025), *Appropriate and Sustainable Alternative Payment Arrangements - Code of Conduct on Mortgage Arrears 2013*.

Back to "Contents"

guidance to avoid future consumer detriment that may arise on the expiry of an alternative repayment arrangement.

From a gatekeeping perspective, incomplete and poor-quality applications for authorisation and controlled function roles can delay the gatekeeping process and the firm's licence approval. Applicants must submit high-quality applications demonstrating effective governance, risk management and internal control arrangements, a sustainable customer-focused business model, and adequate financial and operational resources in line with the Central Bank's Authorisation and Gatekeeping report.[40]

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27
1.1	Assessment of the largest retail credit firms' progress against their **long-term mortgage arrears** reduction targets.	●	●	
1.2	Introduction of an enhanced **sector specific ML/TF Risk Evaluation Questionnaire (REQ)** to capture more detailed and insightful risk data and provide data to the Central Bank to meet new European AML/CFT requirements. *Issued to firms in H2 2026 and expected to be submitted by firms in H1 2027.*		●	●
1.3	Cross-sectoral **thematic review of customer service**, including in the banking and lending sector, a review of the impact of supervisory actions arising from previous reviews.	●	●	
1.4	Cross-sectoral thematic review of the identification and treatment of **customers in vulnerable situations**.	●	●	●
1.5	Cross sectoral review of how firms are carrying out **root cause analysis of errors** and applying learnings to their wider product and service suite.	●	●	

Focus Area 2: Operational and cyber resilience

Weaknesses and immaturity observed in some firms' operational risk management and resilience have come to the fore in recent

[40] See Central Bank of Ireland (May 2025), *Authorisations and Gatekeeping Report 2024*.

Back to "Contents"

years. This has led to instances of service disruption for customers due to system failures and outages. The shortcomings also increase the possibility of customer detriment through the occurrence of successful cyber-attacks, financial scams, fraud and compromised or loss of customer data. The strengthening of operational resilience is a key strategic objective of the Central Bank and planned supervisory activity for 2026 will provide us with an initial overview of the maturity level of the sector. Overall, there is an expectation that firms understand the impacts of operational disruptions, prepare for them and ensure that they can respond to and recover from these disruptions.

Retail credit and credit servicing firms operate in an increasingly complex and interconnected environment across both the retail credit sector and the wider financial sector. The adequacy of firms' investment in technology platforms has consequences for their operational resilience and the quality of their dealings with individual borrowers, which includes customers of other financial institutions. Retail credit and servicing firms are both outsourced service *providers* to other financial institutions and outsourced service *recipients*, primarily from intra-group and external third parties. Outsourcing remains a key sector risk due to some firms' underdeveloped outsourcing oversight and risk management arrangements or poor execution.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26
2.1	Sector specific targeted review of operational resilience incorporating an **operational resilience maturity assessment** to gain an understanding of the level of preparedness and maturity in firms to be able to respond to, recover and learn from operational disruptions.	●	●
2.2	**Industry session** on operational resilience and our expectations for the sector.		●
2.3	Targeted **review of outsourcing registers** to gain an understanding of the firms outsourcing universe and determine levels of interconnectedness across the sector and broader financial system.	●	●

Back to "Contents"

Focus Area 3: Over-indebtedness

Easier access to short-term credit presents a particular risk of consumer over-indebtedness. Financially vulnerable individuals often use short-term credit to a greater extent, more frequently and simultaneously across multiple providers. Its usage can lead to an individual having an inflated sense of available funds leading to an unsustainable level of spending. This is particularly the case with hire purchase, personal contract plans and BNPL products. Recent Central Bank publications in this area have recognised that such offerings can provide flexibility and choice, but if not managed responsibly can carry risks that may ultimately lead to financial difficulty and can harm financial wellbeing. The publications set out our expectations of firms providing such products.[41]

Firms are expected to ensure the effective disclosure of loan terms and conditions (T&Cs) and that borrowers fully understand the nature of the products they are agreeing to. It is particularly important that T&Cs are clear for consumers and that firms recognise and address limitations in some borrowers' understanding of credit. Ensuring consumers are protected against harm or unfair outcomes is at the heart of the Central Bank's work with a number of reviews commencing in 2026.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27
3.1	Cross-sectoral thematic review of **BNPL arrangements**.	●	●	
3.2	Review of **hire purchase terms and conditions**, with an initial desk-based focus.	●	●	
3.3	Cross-sectoral thematic review of **mortgage lending** to include an analysis of credit, loan origination and risks to borrowers (including monitoring for early signs of **over-indebtedness or distress**).		●	●

[41] See Central Bank of Ireland (October 2025), *Who Clicks Pay Later* and *Buy Now, Spend More, Pay Later: Behavioural Mechanisms of Buy Now, Pay Later Products*.

Back to "Contents"

Focus Area 4: Business models and strategy

Although the sector is maturing in many ways, deficiencies remain evident whereby governance, risk management and internal control frameworks have not evolved in line with the scale and complexity of business models. Boards are responsible for the effective, prudent and ethical oversight of their firms. They are responsible for, among other things, setting and overseeing the business strategy, the implementation of effective risk management and internal control frameworks, and ensuring that firms have the financial and operational capacity to deliver their business strategies.

With loan books maturing, firms must focus on the sustainability of their business models over the short-to-medium term, with boards owning and implementing strategies to secure an ongoing path to profitability. The significant decrease seen in the level of non-performing loans (NPL) on lenders' balance sheets and loan sales is leading to lower assets under management in the retail credit sector, with fewer portfolio sales and reduced credit-servicing opportunities in the market. In addition, firms have experienced higher-than-expected run-off rates as borrowers took advantage of the lower interest environment. This erodes revenues against largely fixed cost bases, with squeezed margins as a result.

From the perspective of the safety and soundness of firms, the challenging external environment may lead to higher funding costs impacting their ability to lend at competitive rates and grow their business. This is particularly the case for active lenders and relates to both firms reliant on parent groups for ongoing investment support and those raising funds in external markets. Firms should ensure they have considered their funding strategies and that such strategies can credibly support the delivery of a sustainable business model which has the interests of customers at its heart.

The high-cost credit sector has faced challenges in recent years which have seen several exits from the market. To strengthen consumer protections, an interest rate cap was introduced by the Oireachtas under the Consumer Credit (Amendment) Act 2022.[42] As provided for under the Act, the Central Bank subsequently undertook an assessment of the cap's impact, and we issued our report in January 2026. The assessment concluded that the cap was

[42] The objective of the interest rate cap was to protect consumers from excessive borrowing costs. A cap of 1% per week up to a maximum of 48% applies on fixed rate loans, with a 2.83% nominal interest rate on the outstanding balance per month on running accounts.

Back to "Contents"

effective in reducing interest rates as intended and strengthened consumer protections without significantly adversely affecting competition or financial inclusion. While credit supply remained steady, the cash loan sector declined with shorter-term loans becoming less available. The consumer research we undertook and our engagement with civil society bodies highlighted that the sector remains important for providing regulated credit to underserved borrowers.[43]

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27
4.1	Cross–sectoral review of data collections to ensure all reporting requirements have a clear purpose. Industry engagement to commence on our **review of existing Conduct of Business Returns**.	●	●	●
4.2	Targeted sectoral assessment of **business model viability and sustainability** of the sector.	●	●	

[43] See Central Bank of Ireland (January 2026), *Review of Interest Rate Cap on High Cost Credit*.

Back to "Contents"

Credit Union Sector

KEY TAKEAWAYS

- Credit unions must continue to better understand and mitigate their financial, operational and cyber risk exposures and address structural vulnerabilities and organisational deficiencies, so that they are able to effectively navigate the unstable, fast-moving and technology-driven operating environment. The Registry of Credit Unions engaged with credit unions in 2025 in relation to actions required to address supervisory concerns and mitigate risks.
- Legislative and regulatory change over recent years is enabling credit unions to increase lending (including longer term loans) and to collaborate and further develop their business model in a prudent manner. While there are some emerging signs of sectoral collaboration, the challenge remains for individual credit unions and the sector to leverage the opportunities arising to develop and implement a coordinated sectoral strategy.
- As credit unions have increased the range of products and services offered to members, it is now appropriate to apply the Consumer Protection Code 2025 to all regulated activities, to ensure that credit union members are afforded the same consumer protections as other financial services consumers.

Sector Profile

- Credit unions are community-based and member-focused, supported by a mutual structure.
- 172 active credit unions in Ireland, a decrease of over 80 from eight years ago. Key metrics (30 September 2025):
    - 3.7m members (End of 2024: 3.7m)
    - €18.7bn savings (End of 2024: €18.1bn)
    - €7.7bn gross loans (End of 2024: €7.1bn)
    - €13.9bn investments (End of 2024: €13.7bn)
- Significant changes have taken place in the sector, supported by an updated legislative and regulatory framework. Sector restructuring continues to improve sustainability, create scale and help address organisational weaknesses.

Back to “Contents”

Our supervisory approach to the sector

Our supervisory activities and interventions are undertaken on a sectoral basis, with credit union specific engagement where appropriate. Planned activities include the ongoing analysis of data and regulatory returns, assessments of the ownership of IT risk and IT outsourcing risk, monitoring of liquidity and asset and liability management (ALM) and thematic reviews in specific risk areas including credit risk.

Sectoral assessment and supervisory focus areas

Focus Area 1: Financial resilience

Credit unions have demonstrated resilience in the face of the systemic shocks and heightened volatility of recent years. Sectoral reserves and liquidity remain strong, with surpluses reported across the sector in the financial year ended 30 September 2025**.** Given that the funding base of credit unions is largely demand savings, liquidity risk will increase where credit unions increase their longer-term lending. ALM should reflect projected inflows, outflows and maturities as well as ensuring resilience to withstand liquidity stress scenarios. Maintaining and building adequate levels of reserves, including adequate operational risk reserves, also remains key to ensuring credit union financial stability and resilience.

Longer term sustainability challenges remain, notably the sector's continuing low loan to asset ratios, albeit these have been increasing marginally. It is our expectation that credit unions planning to avail of the changes afforded by the new lending framework do so in a phased, prudent and sustainable manner. Credit unions are also expected to continue to develop the skills, expertise and risk management necessary for house and business lending. More broadly, geopolitical and geoeconomic events will continue to present a risk to credit quality and investment valuations.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
1.1	Monitoring of **liquidity and ALM** supported by data and appropriate KRIs, with targeted follow up where breaches or adverse trends are identified.	●	●	●	●

Back to "Contents"

		H1 26	H2 26	H1 27	H2 27
1.2	Engaging with the sector on the roll out of the **updated Prudential Return** including supervisory follow up in relation to quality of data submitted.	●	●	●	●
1.3	Provision of statistical data to credit unions.	●		●	●
1.4	Analysis of **credit risk, loan origination and risks to borrowers** (including monitoring for early signs of over-indebtedness or distress).	●	●	●	●

Focus Area 2: Operational and cyber resilience

As credit unions enhance member offerings, including online services and current accounts, the importance of technology and digitalisation is evident. Members expect access to their funds 24/7, including the ability to transfer funds and make instant payments. A severe business interruption has the potential to adversely impact the continuity of services to members. Credit unions, like other firms in the system, are also exposed to the increased frequency of cyber-attacks across the financial sector. Accordingly, credit unions are expected to have adequate processes in place to effectively manage and mitigate IT security and cyber risk, including where information security processes are outsourced.

The Central Bank's IT thematic review conducted last year in the credit union sector assessed IT risk management, internal controls and governance. Details of the findings and expected follow up actions were communicated to all credit unions. It is the responsibility of credit union boards to *"develop, prepare, implement and maintain secure and reliable information systems"*.[44] Credit unions are required to have adequate IT governance and risk management processes to effectively mitigate their IT risks and the risks associated with the outsourcing of IT services, including cloud services. Where fully embedded this enables the identification, assessment and appropriate mitigation of IT risks, while maintaining the continuity of member services. This will also support the

[44] In accordance with Section 76G of the Credit Union Act 1997 (Information Systems)

Back to "Contents"

operational resilience of credit union IT systems and the security of member data.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
2.1	Validation of **Risk Mitigation Programmes** issued to specific credit unions arising from the thematic review of **IT risk**.	●	●	●	●
2.2	Engagement with credit unions on required actions to demonstrate **ownership and stewardship of IT risk** including IT outsourcing risk, as highlighted in the thematic review of IT risk.	●	●	●	●
2.3	Engagement with sector stakeholders in relation to credit unions' preparation for the **application of the Digital Operational Resilience Act (DORA) from January 2028**. *(Expected completion H2 2028.)*	●	●	●	●

Focus Areas 3: Business model and strategy

Significant change in the credit union sector has been driven by consolidation and the provision of a broader range of products and services to their members. In addition, over the last decade there have been significant changes in the legislative and regulatory framework which enables credit unions to do more within appropriate limits and guardrails.

Credit unions still need to demonstrate the necessary focus on strategic transition aligned with their risk appetite and tolerance. The sector is at risk of not keeping pace with digitalisation and meeting members' needs and expectations, nor taking advantage of the opportunities provided through legislative and regulatory changes. Credit unions are expected to further collaborate in the development and implementation of a coordinated strategy.

The main planned activities relating to this supervisory focus area are:

Back to "Contents"

		H1 26	H2 26	H1 27	H2 27
3.1	Supporting strategic restructuring activities for **Transfer of Engagement (TOE)** projects by credit unions, with enhanced post transfer oversight for large scale TOE projects.	●	●	●	●
3.2	Establishment of a **regulatory framework for investment in credit union shared service organisations**. – Consultation paper – Introduction of the regulation	●	●		
3.3	Establishment of a **regulatory framework for corporate credit unions:** – Research and policy formulation commencing – Consultation and introduction of regulations: 2027-2028	●	●	●	●
3.4	Engagement with Department of Finance on its development of a **Strategy for the Credit Union Sector** (2025 Programme for Government commitment).	●	●		
3.5	Publish a **Credit Union Engagement Charter** setting out principles for, and information on, the Registry's direct engagement with credit unions. Engagement with credit unions on **collaboration initiatives**.	● ●	 ●	 ●	 ●

Focus Area 4: Culture, governance and risk management

Protection by each credit union of the funds of its members and the maintenance of the financial stability and well-being of credit unions generally is enshrined in our statutory mandate. Arising from the changes in the legislative and regulatory framework for credit unions, which enables the sector to do more within appropriate limits and guardrails, the Central Bank believes it is now appropriate to apply the Consumer Protection Code 2025 to all regulated credit union activities. This will ensure that credit union members are afforded the same consumer protections as other financial services consumers.

In advance of the application of the Consumer Protection Code, credit unions are expected to manage conduct risk and demonstrate the protection of their members' interests. They should address any conduct matters arising in a member-centric

Back to "Contents"

manner. Upon the commencement of the Code, credit unions will be expected to be able to demonstrate that members are at the forefront of their considerations when they are evolving or developing their business model and strategies.

As credit unions offer more products and services they need to mature their risk management, control frameworks and capabilities to provide products and services safely and to ensure these frameworks adequately address the evolving nature of risks arising. Notwithstanding that inherent money laundering and terrorist financing risk in this sector remains low, credit unions must strengthen their capacity to identify and manage emerging ML/TF and other financial crime risks from business development activities.

Deficiencies in data capabilities may undermine a credit union's understanding of their risk exposures and lead to blind spots and poor decision making. This includes poor data quality and a lack of robust data reporting and disclosure. Credit unions are expected to have adequate processes and systems in place to ensure data frameworks are robust and support accurate and timely internal risk reporting, regulatory reporting and decision making.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
4.1	Engagement with the sector on the planned application of the revised **Consumer Protection Code** to all credit union activities, to ensure their members are afforded the same protections as other consumers. The public consultation process will close in March 2026, and it is intended to have regulations published by end Q3 2026.	●	●	●	●
4.2	Credit unions will be required to complete an **enhanced Risk Evaluation Questionnaire (REQ)**. The enhanced REQ will capture detailed quantitative and qualitative risk information on **ML/TF risk** and the quality of **AML/CFT controls**. This data will be used to: (a) identify firm and sector-specific issues and emerging trends; (b) guide supervisory strategy; and (c) satisfy incoming data requirements for the EU's Anti-Money Laundering Authority (AMLA).		●	●	●

Back to "Contents"

Insurance & Reinsurance

Back to “Contents”

Insurance and Reinsurance Sectors

KEY TAKEAWAYS

- While the Irish insurance sector has maintained a stable and robust solvency position in recent years, (re)insurers are operating in an increasingly challenging and volatile macroeconomic and geopolitical environment.
- Prudent and fair pricing, robust underwriting and reserving practices, capital adequacy, effective model risk management and operational resilience are fundamental to the insurance sector's continued safety and soundness.
- Building consumer trust and confidence in providers and insurance products remains critical to the effective functioning of the market. Insurance products should be well-designed and deliver the intended benefits and value to consumers.
- Firms must ensure that technological adoption strengthens rather than undermines their ability to price fairly, reserve adequately and treat customers appropriately.
- Firms must be ready to implement changes to legislation that will be effective over the course of 2026/2027. Revisions to the Consumer Protection Code, the Solvency II Framework and the EU-wide Recovery and Resolution Directive for (re)insurers will all come into effect.

Sector profile

- Ireland has the fourth-largest life and non-life insurance sector in the EU measured by gross written premium (GWP).[45]
- Over 170 (re)insurance firms are authorised in Ireland, the majority of which are subsidiaries of large international groups. These include life insurers predominantly focused on unit linked investment and pensions saving products and protection products, with non-life insurers and reinsurers offering cover ranging from personal motor, household and health insurance to specialty insurance such as cyber and marine. Captives provide non-life insurance solely to the group to which they belong.
- • Irish (re)insurers provide cover to 20m insurance consumers in Ireland and globally. Domestically, there are some 2.5m private motor insurance policies, 2.7m life insurance and pension policies

[45] See EIOPA (November 2024), *European Insurance Overview 2024*

Back to "Contents"

and 2.5m people with health insurance cover.[46] Approximately 70% of the €109bn GWP in 2024 was international business and came from over 70 countries.

- Ireland is home to a growing number of Insurtech firms, which aim to leverage artificial intelligence and other advanced technologies to disrupt the traditional insurance industry.

Our supervisory approach to the sector

We supervise the (re)insurance industry through a mixture of sectoral and firm-specific work. Each firm within the insurance industry is classified into one of four sectors – domestic life insurance, domestic non-life insurance (including health), reinsurance (including captives) and international insurance (life, non-life and specialty). Supervisory activities will include direct engagement with firms and individuals on our prioritised risks, cross-sectoral risk assessments, sectoral thematic reviews, onsite inspections, monitoring and review of submissions (e.g. regulatory returns) and cross-industry engagement via supervisory questionnaires. Our supervisory activities will include supporting the delivery of EIOPA's Union-wide strategic supervisory priorities.[47]

We will continue to enhance the effectiveness and efficiency of our regulatory and supervisory work and remain actively engaged in international simplification discussions through engagements with EIOPA and the other EU supervisory authorities. We have already identified areas where we could simplify and reduce the burden for the industry. Examples of changes already implemented include the streamlining of authorisation and change of business requirements for firms and the removal of the requirement for an external audit of captive insurers' regulatory returns and public disclosures.

We continue to focus on improved transparency around the claims environment. This is through the National Claims Insurance Database (NCID), which provides tracking of claims trends, legal costs and insurer profitability, helping to identify cost drivers and to support evidence-based policymaking. Also, through our regular reports and data sets containing analysis of the costs of claims, the cost of premiums and the costs of settling claims.

[46] See Millman for Insurance Ireland (September 2025), *Resilience & Revitalisation: Shaping the Future of Insurance*
[47] See EIOPA (September 2025), *Union-Wide Strategic Supervisory Priorities*.

Back to "Contents"

Throughout 2026, we will continue to work and engage with industry on the implementation of the Solvency II reforms (see Box 3). This will include an industry questionnaire and the development of processes to assess small and non-complex undertaking (SNCU) notifications and applications by firms to avail of proportionality measures. Dedicated sectoral engagement is planned to support the successful implementation of the changes, which will include industry webinars and regular updates in our insurance publications.

Box 3: Changes to Solvency II Regulations

The existing Solvency II regime, introduced in 2016, has been amended (Directive (EU) 2025/2) and will come into effect from January 2027. Some firms, in particular small and non-complex undertakings (SNCU), may be able to avail of reduced regulatory reporting requirements.

Early insights from supervisory engagements last year indicate that most firms have carried out an initial impact assessment of the material changes. A questionnaire will issue to all (re)insurance firms (excluding captives) in Q1 2026, to gain greater understanding of how individual firms and overall sectors will be affected by the changes and the proportionality measures that firms may apply for.

Based on the results of the questionnaire and our engagement with industry we may develop a pre-application process for firms that are not SNCUs that wish to apply for proportionality measures as allowed for under the Directive. This would provide firms with an opportunity to engage with the Central Bank in advance of a formal application phase in 2027. Participation in the pre-application process would be voluntary for firms, noting that the Central Bank cannot take a decision on an application until after the relevant amendments to Solvency II have come into force.

Over 2026, it will be important for firms to fully prepare for the implementation of the regulatory changes to ensure compliance with the amended regime from January 2027.

The EU Insurance Recovery and Resolution Directive entered into force on 28 January 2025, with full implementation required by 30 January 2027. The Central Bank will support industry in establishing the necessary recovery planning and resolution capabilities to strengthen financial stability and protect policyholders.

We will also continue to engage across the insurance industry and at an individual firm level on the implementation of the revised Consumer Protection Code. Building on the revised Code we will review the current Conduct of Business Returns for insurance firms,

Back to “Contents”

to better reflect priority risks and enhance reporting on consumer risks across the sector. Guided by our approach to simplification, we will work to identify areas that require updates, targeted additions validated by robust analysis and removal of requirements that are no longer applicable.

Sectoral assessment and supervisory focus areas

Focus Area 1: Treatment of customers

Insurance serves a critical role in reducing uncertainty by protecting people and businesses against the risks of adverse future events. Consumers rely on insurance to provide support in the event of loss or serious accident, to plan for retirement, to enable them to confidently invest in and run their businesses and more. Building consumer trust and confidence in the insurance industry and in insurance products remains critical to the effective functioning of the market. Consumers need to trust that insurers are providing products that are suitable and at a fair price, that adequate customer service and support will be provided when needed, and that firms will honour the commitments they have made where insured risks crystallise and claims occur. A lack of consumer focus when providing insurance products, including deficient practices, processes and systems, or inadequate levels and experience of staff, can lead to poor outcomes for consumers.

Insurance firms must ensure that all products, regardless of the jurisdiction in which they are sold, are designed, approved and monitored, and continue to meet target market needs and deliver good customer outcomes. Firms must implement product oversight and governance policies, involving oversight by senior management, ensuring products are suitable, provide value for money and are distributed appropriately, avoiding detriment throughout their lifecycle. This is particularly important where products are more complex or where suitability may change over time based on consumers' circumstances, for example, longer-term life insurance products, or where there are many similar types of products to choose from such as in the health insurance market. The Central Bank commenced product oversight and governance reviews last year on the domestic health insurance market (with feedback due to issue to firms in H1 2026) and on the international insurance sector, with work in this sector continuing throughout 2026.

Back to "Contents"

Well-designed products, with clear information, are essential to ensure consumers choose the most suitable products and get the intended benefits and value. Firms must ensure that the information provided to customers is clear and presented in a way that informs the customer of all relevant material information, including the benefits and exclusions related to each product. A failure to give clear information to consumers at any point in the life of a product or service will affect the consumer's ability to make informed decisions. This could result in harm to the consumer. For example, it could result in them failing to properly provide for their future needs, paying more for a service than they need, or paying for a financial service that they do not require. It is also key that firms explain what a product does not do, or what it excludes. An example of work we have undertaken in this area relates to customer communication on No Claims Discounts (NCDs) in the domestic non-life sector. This thematic review is nearing completion and findings will issue to firms in Q1 2026.

Affordability and access challenges occur against a backdrop of increasing premiums that could lead to lapses, reduced coverage and availability, and widening protection gaps. This is particularly apparent in products such as motor, home/property, public liability and health. A concerted focus on effective solutions to protection gaps, including flood risk, is essential. We will continue to engage with the insurance industry and other key stakeholders, building on detailed research into the nature and scale of the flood protection gap in Ireland undertaken in in recent years.[48]

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
1.1	Thematic review of **customer service levels in the domestic non-life sector** and **complaints handling in the domestic life and domestic non-life sectors**. *(Continued from 2025)*	●	●		
	Thematic review of aspects of **new business administration processes in the domestic life sector** with a focus on the adequacy of internal controls to ensure that policies are issued in line with requirements. *(Continued from 2025)*	●	●		

[48] See Central Bank of Ireland (October 2024), *Flood Protection Gap Report*.

Back to "Contents"

		H1 26	H2 26	H1 27	H2 27
	Thematic review in the **domestic life sector** of how customers are being **informed** effectively.	●	●		
	Thematic review of the identification and treatment of **vulnerable customers in the domestic life sector**.		●	●	
1.2	Cross-sectoral review of a range of **commission arrangements** in the sale of products and services to customers through intermediaries, to understand how they are working to secure customers' best interests, to include engagement with, and data gathering from, product producers and providers.		●	●	●
1.3	Thematic review of **product oversight and governance in the international insurance sector** which will include a particular focus on value for money for certain product types. *(Continued from 2025)*	●	●		
1.4	Thematic review of certain **in-force business administration processes** including: – **claims handling in the domestic non-life sector**, with a focus on consumer outcomes and consideration of vulnerability, and – **claims, surrenders and switches in the domestic life sector**, with a focus on service levels, consumer outcomes and customer centricity.		●	●	
1.5	Support the implementation of the Government's Action Plan for Insurance Reform 2025-29, with significant work planned under the themes of ***Transparency and Affordability*** and ***Climate Protection***.[49]	●	●	●	●

Focus Area 2: Financial resilience

While the Irish insurance sector has maintained a stable and robust solvency position in recent years, (re)insurers are operating in a challenging and volatile macroeconomic and geopolitical environment. Given the industry's broad international footprint, there is a heightened exposure to geopolitical change. This creates a key source of uncertainty for pricing, underwriting and reserving

[49] Government of Ireland (July 2025), *Action Plan for Insurance Reform 2025-29*.

Back to "Contents"

practices and underlying business models. (Re)insurers need to be aware of and manage the potential adverse macroeconomic or macrofinancial impacts that include: inflation spikes that drive increases in the costs of (re)insurance claims and operating expenses; corrections and volatility of global financial markets, leading to investment losses; direct insurance losses on certain lines of business; and reduced economic activity affecting the demand for insurance. Since these risks typically share common geopolitical drivers, they may occur simultaneously, amplifying the potential impact on firms' capital positions.

Prudent pricing, underwriting and reserving practices remains critical for the safety and soundness of the (re)insurance industry. The financial resilience of (re)insurance firms depends on disciplined approaches to both setting premiums and establishing reserves that are adequate to meet future claims obligations. History demonstrates a clear pattern whereby failures in pricing discipline or inadequate reserving practices often precede financial distress in firms and cause consumer harm. We continuously monitor and engage with firms on these risks, recognising that pricing, underwriting and reserving decisions made today determine whether firms can meet their obligations in the future.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26
2.1	**Solvency II Review survey** will issue to all (re)insurance firms (except captives), focusing on the expected impact of Solvency II changes, and to ascertain how many firms intend to apply for proportionality measures. Based on the results of the questionnaire we may develop a pre-application process for firms that are not SNCUs that wish to apply for proportionality measures. *Questionnaire issued in H1 2026 followed by assessment and engagement in H2 2026.*	●	●
2.2	Supervisory review of **investment risk in the domestic non-life sector**, to assess appropriate consideration of, and responsiveness to, geopolitical risks, including through effective oversight of investment portfolios.	●	●

Back to "Contents"

		H1 26	H2 26
2.3	**Monitoring of resilience across all sectors** through assessment of stress scenarios and analysing and engaging with firms on material changes in the external environment.	●	●
2.4	Cross-sectoral review of **pricing, underwriting and reserving practices for international and reinsurance firms** in the context of heightened geopolitical risks, market softening and other risk factors.	●	●

Focus Area 3: Digitalisation and artificial intelligence

The insurance sector is undergoing significant digitalisation, with firms increasingly adopting advanced technologies to improve internal efficiency and customer experience. Our engagement with the insurance industry, including a 2025 survey on the use of AI, has shown that most firms are already using AI, and GenAI in particular, or intend to start using AI soon. Consistent with findings at European level, Irish (re)insurance firms point to the benefits of streamlining operations, enhancing data analysis and improving pricing accuracy.[50] Adoption of these new technologies introduces additional operational and consumer risks that firms must carefully manage.

The adoption of AI systems presents challenges. AI has the potential to enhance pricing models and claims assessment, but without appropriate controls, these systems could introduce discrimination, lack of transparency, or exclude vulnerable consumers. If AI systems are permitted to operate without adequate human oversight, firms risk making pricing or claims decisions that are neither fair nor explainable to consumers. Data management, privacy and security vulnerabilities can also arise, particularly where firms lack sufficient technical expertise or governance frameworks to manage these systems responsibly.

Firms must ensure that technology adoption strengthens rather than undermines their ability to price fairly, reserve adequately, and treat customers appropriately. This requires robust governance, clear accountability, oversight and monitoring. Firms must navigate the potential risks and implications from increasing digitalisation and

[50] See EIOPA (February 2026), *EIOPA survey on Generative AI shows swift but cautious adoption among Europe's insurers*.

Back to "Contents"

analytical technologies throughout the insurance sector in a manner that places the best interests of consumers at the heart of their business models and decision-making. We will continue deeper and more focused engagement throughout 2026 in this space, so that innovation serves both financial stability and consumer protection alongside other business purposes.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26
3.1	Engagement with individual firms on their **current use of and strategy for AI** to further understand the potential impact on business models and associated risks.	●	●
3.2	Stakeholder engagement, aligned with the Central Bank's approach to **innovation in the sector**, with a particular focus on supporting innovation that meets the evolving needs of households and businesses while ensuring rigorous oversight.	●	●
3.3	Supporting the effective **implementation of the EU AI Act** and incorporation within supervisory strategies across all insurance sectors.	●	●

Focus Area 4: Climate change and sustainability

(Re)insurers face direct and indirect exposures to climate change risks across three dimensions: physical risks from extreme weather events, transition risks from the shift to a low-carbon economy and litigation risks from climate-related disputes. The nature and magnitude of these exposures vary according to the types of risks firms cover and their geographical footprint. For primary insurers, these exposures are compounded by changes in reinsurance capacity, terms and pricing. As reinsurers reassess their climate risk exposure and adjust their offerings, primary insurers face constraints on the coverage they can provide and the terms they can offer consumers. This creates a cascading effect across the sector, with implications for both resilience and consumer access to insurance, potentially widening the protection gap for certain consumers.

Climate and sustainability risks have long-term effects that extend far beyond individual underwriting cycles. Recent supervisory work has demonstrated that many firms have not sufficiently integrated

Back to "Contents"

these risks into their core risk management and governance frameworks or their strategic planning. Firms must continue work on embedding climate risk into underwriting practices, pricing and reserving models and capital planning.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26
4.1	Cross-sectoral review of how **international insurance and reinsurance** firms have integrated **climate change risks** into their **business model**, **strategy** and **underwriting practices**.		●
4.2	Focused engagement with and provision of support to stakeholders in the development of a long term and sustainable approach to addressing **climate protection gaps**, particularly for **flood insurance risk** in Ireland.	●	●
4.3	Monitoring (re)insurance firms' progress on the integration of **climate change risks** into their **risk management** and **governance frameworks** and assessment of climate change risk.	●	●

Focus Area 5: Operational and cyber resilience

Analysis of outsourcing arrangements demonstrates that some insurers have developed significant reliance on third-party or group service providers for key activities. This includes information and communication technology (ICT), policy administration, claims management, underwriting support and investment management. Whilst outsourcing can provide operational efficiencies, it also transfers operational risk to external parties and creates dependencies that must be actively managed. We expect firms to maintain clear visibility and control over outsourced functions, with robust contractual arrangements, performance monitoring and contingency plans. Firms must also ensure they have appropriate oversight of the sub-outsourcing arrangements of their key service providers, as risks may be transmitted via this channel. When firms depend heavily on group support, they may lack the capability to operate effectively if conflicts of interest arise between group and local entity priorities.

Attention is required in relation to critical or important business services (CIBS). Disruption to these services, whether through cyber-

Back to "Contents"

attack, operational failure or service provider insolvency, could impair a firm's ability to serve customers or meet regulatory obligations. Firms must ensure that critical services have appropriate redundancy, business continuity arrangements and oversight in place.

Cyber-attacks give rise to significant operational risks for firms, as well as the risk of loss or misuse of customer data. The expansion and integration of technology into business models also exacerbates governance, control and oversight risks for firms in several areas. Although the impact of cyber disruptions has so far been limited in duration and scope, this may not always be the case. Mitigation of cyber risk requires effective risk management frameworks and executable contingency plans covering both their own operations and their outsourced service providers. When incidents occur, firms must consider the impact on their customers and communicate in a timely and transparent manner. This is essential to maintain customer confidence and demonstrate that operational resilience is embedded throughout the organisation.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
5.1	Thematic **review of domestic non-life insurers to assess ICT risk management** as part of a firm's overall risk management system in order to assess digital operational resilience and embeddedness of the DORA framework. *Continuing from 2025. This review is ongoing with certain firms selected each year for review.*	●	●	●	●
5.2	Thematic review of **operational resilience in the international insurance sector**, to assess the progress that firms have made against the Central Bank's **Cross-Industry Guidance on Operational Resilience**.	●	●		
5.3	Thematic review of **operational resilience in the domestic life sector**, with a focus on the Pillar 2 "respond and adapt" element of the Central Bank's **Cross-Industry Guidance on Operational Resilience**.		●	●	

Back to "Contents"

Markets & Funds

Back to “Contents”

Funds Sector

KEY TAKEAWAYS

- The Irish funds sector is operating in a fast-evolving landscape facing into a sustained period of transformation across many aspects including geopolitical fragmentation, evolving regulation, business model adaptations, increases in complex product offerings and digital transformation.
- Simplification and the Savings and Investment Union (SIU) will be central to improving EU competitiveness and the financial wellbeing of EU citizens. The Irish funds sector has a pivotal role in supporting the success of these key EU initiatives.
- The size and ever-increasing complexity of the sector present a broad range of risks to the Central Bank's safeguarding outcomes which require continuous monitoring and oversight. This includes our ongoing and robust supervision of fundamental risks such as liquidity, leverage coupled with an enhanced focus on private (complex) assets, anti-money laundering practices, the impact of digitalisation and asset valuation.
- As such, the effectiveness of governance, risk management and operational resilience frameworks across the funds sector remains a priority in 2026 and beyond.

Sector profile

- Ireland is a significant global funds domicile, with 136 regulated fund management companies (FMCs) and 65 fund service providers (FSPs) including 41 fund administrators and 24 depositaries offering services to funds and investors globally as well as domestically.
- Approximately 9,100 funds are authorised in Ireland with net asset value (NAV) of almost €5.3tn in September 2025 (an increase of 6% on end 2024).[51]

[51] Two main categories of funds authorised by the Central Bank are UCITS (Undertakings for Collective Investment in Transferable Securities) which mainly invest in securities such as equities and bonds, and AIFs (Alternative Investment Funds) which can invest in alternative assets such as commercial real estate.

Back to "Contents"

- Ireland is also host to two-thirds of the total assets of the Exchange Traded Funds (ETFs) sector in the euro area with total net asset value (NAV) of over €1.9tn in September 2025.

- Environmental, social and governance (ESG) funds represented 32% by fund count (2,878) and 39% by net asset value (NAV) (€2.07tn) of all Irish funds at September 2025.

Our supervisory approach to the sector

The Irish funds sector is operating in a fast-evolving landscape facing into a sustained period of transformation across many aspects including geopolitical fragmentation, evolving regulation, business model adaptations, an increase in complex product offerings and digital transformation. Our supervisory activities across the funds sector will be undertaken at firm level for those subject to close and continuous supervision and sectoral level for others supplemented by firm specific work as appropriate.

Planned activities are set out below and cover seven focus areas. These include thematic reviews across a range of risk areas with a particular focus on the effectiveness of governance including delegation and outsourcing frameworks, oversight and control of cyber and operational resilience, liquidity and leverage risk, asset valuation and market risk management.

The outcomes we aim to achieve are linked directly to these risks and focus on ensuring the integrity of the market with well-governed and resilient firms, effective safeguarding of client assets, securing investors' interests, transparent disclosure and high standards of compliance with applicable rules. Regulation and supervision play a vital role in supporting well-functioning markets. It ensures the protection of investors and mitigates the risks to both the resilience of management and servicing firms operating in the sector, and to financial stability more broadly. In addition, the Central Bank will engage closely with the European Securities and Markets Authority (ESMA) to achieve convergence on supervisory matters across the sector through participating in common supervisory actions (CSAs), peer reviews and voluntary supervisory colleges.

Back to "Contents"

Sectoral assessment and supervisory focus areas

Focus Area 1: Governance and risk management

Deficiencies in governance and risk management practices can affect the operational soundness of firms and increase the likelihood of investor detriment. Where robust governance and risk management frameworks are not in place, this negatively impacts the oversight and control of the funds under management, ultimately resulting in the potential of adverse impacts for investors.

A key governance risk arises when local boards or executive committees have insufficient substance or have inadequate decision-making and management capacity. As with other sectors, this risk may be heightened where there are diverging cultural values or geopolitical positions between parent and local entities. Similarly, risk management frameworks may be constrained if local entities lack the capacity to set and manage their own risk appetite. Weaknesses in risk monitoring, compliance functions or the implementation of the three lines of defence model increase concerns about effective oversight, particularly for delegated activities and outsourced service providers. The scale of these arrangements adds complexity to risk management.

Tone from the top shapes organisational culture and when commercial objectives overshadow investor protection and conduct risk it may result in poor outcomes, particularly for retail or vulnerable investors. Without strong leadership messaging and accountability, operational inefficiencies and compliance failures are more likely to go undetected or unresolved, potentially causing harm to investors.

Our approach to assessing governance risk in 2026 will be through sectoral reviews focusing on themes such as delegation, board effectiveness and depositary oversight of fund managers. The effectiveness of related governance and controls in place will be a key input into how we conclude these reviews and identify next steps for the funds sector.

The main planned activities relating to this supervisory focus area are:

Back to “Contents”

		H1 26	H2 26	H1 27	H2 27
1.1	Continuation of our sectoral assessment of **delegation in fund management companies (FMCs)** with the first industry communication from the review in H1.	●			
1.2	Conclude our review of the **effectiveness of fund administration and depositary management of outsourcing**.	●	●		
1.3	Review of **governance and board effectiveness in fund administrators and depositories**.		●	●	●
1.4	Review of **compliance functions across fund administrators and depositaries**. *(Commencing engagement in H1 2026)*	●			
1.5	**ESMA Common Supervisory Action.** *(Subject area will be confirmed by ESMA in due course.)*	●	●	●	●
1.6	Supporting the **transition to AIFMD II** for funds and fund service providers.	●	●	●	●

Focus Area 2: Operational and cyber resilience

Deficient cyber risk frameworks and weak operational resilience structures can increase the likelihood of service disruption and attacks on firms and their third-party digital providers. The volatile and unpredictable geopolitical backdrop heightens the risk of such events. These incidents can compromise critical and important functions, heighten the risk of personal data loss or misuse, and disrupt investment services, leading to harm for consumers and investors. Strong operational risk management, including scenario testing and business continuity planning, is necessary to mitigate threats from cyber incidents, natural disasters and power outages.

While outsourcing can deliver efficiencies, an overreliance on external providers can dilute local management's control over key activities. High levels of delegation and outsourcing across the funds sector can present challenges to the maintenance of control over risk and portfolio management, business continuity, the application of AI processes and cyber security. Robust due diligence, governance and ongoing oversight are essential to manage concentration, dependency and conduct risks.

Back to "Contents"

As noted in the banking sector section earlier in this report, the impact of CRD6, which comes into effect in January 2027, will result in material business model restructuring for financial groups engaged in cross border core banking activities. This includes existing Irish depositary businesses with global custody operations, or more specifically, to their related banking activities which are required to deliver those custody services to Irish funds. While the extent of the impact and the related restructuring required continues to be assessed by many firms, any authorisations and related plans will need to be successfully executed in 2026 to ensure compliance with CRD6. We expect this is a key strategic focus for those impacted firms and therefore the related regulatory engagement required remains a core priority in 2026.

Across the funds sector, financial crime risk continues to require attention. Funds can be exploited for money laundering and terrorist financing, with the funds sector in Ireland being the subject of international scrutiny from an AML/CFT perspective given its size and reach. It is a key area of focus for the Central Bank and, in 2026 for example, we will be undertaking a thematic review of suspicious transaction report (STR) reporting in the sector. Inadequate monitoring of these risks exposes the sector to potential abuse, including breaches of financial sanctions. Furthermore, weaknesses in IT systems and controls can increase investor vulnerability to fraud, scams and misuse of personal data, especially as technological innovations continue to evolve rapidly.

The main planned activities relating to these supervisory focus areas are:

		H1 26	H2 26
2.1	Focus on FMC and FSP implementation and monitoring of the requirements of **DORA** including **threat-led penetration testing**. *Survey issued in H1 2026.*	●	●
2.2	A risk-based approach to AML/CFT/FS will continue into 2026 through supervisory data requests including the **new, enhanced Risk Evaluation Questionnaire (REQ)**. The enhanced REQ will capture detailed quantitative and qualitative risk information on ML/TF risk and the quality of AML/CFT controls. This data will be used to: (a) identify firm and sector-specific issues and emerging trends; (b) guide supervisory	●	●

Back to "Contents"

		H1 26	H2 26
	strategy; and (c) satisfy incoming data requirements for the EU's Anti-Money Laundering Authority (AMLA).		
2.3	A thematic inspection focused on **transaction monitoring and STR reporting** and engagements with firms across the sector.	●	●
2.4	Engagement on the execution by impacted **depositaries** of their **CRD6 compliance plans**.	●	●

Focus Area 3: Asset valuation and market risks

Equity markets, particularly large-cap growth stocks, are trading at elevated levels supported by strong sentiment, creating vulnerability to correlated sell-offs. Narrow credit spreads reflect similar risk appetite across both asset classes. Increased geopolitical and tariff risks are likely to see spreads widen in the long run. Private credit and private equity valuations remain opaque, with limited observable inputs relying on models and professional judgment that may not reflect true economic value. For domestically focused commercial real estate funds, the Irish commercial property market continues to stabilise with capital values in industrial and retail returning to growth in 2025 and sentiment indicators pointing to further recovery.

Funds must accurately value all portfolio assets including those without readily available market prices. Incorrect valuations can cause investors to overpay or receive less at redemption whilst also harming remaining investors. Funds that invest in less liquid (for example, real estate, private equity or private credit) or complex assets (for example, collateralised loan obligations) are more susceptible to this risk due their reliance on potentially outdated prices, statistical models and expert judgement. Optimistic pricing and underestimation of market risks may expose investors to higher risks than intended and reduce financial resilience. The increase in private asset strategies and distribution channels (such as platforms) heightens the need for effective, consistent and well-evidenced valuation practices.

Our supervisory focus will remain on valuation governance and financial resilience where uncertainty is greater. In 2026 we will undertake a thematic review focusing on hard-to-value assets,

Back to “Contents”

reviewing policies, models and controls for level 3 assets (including real estate, private equity, private credit and other illiquid securities) across selected Irish authorised funds, managers and depositaries. This will be complemented by ongoing risk-based engagement relevant to specific cohorts of funds along with reactive supervisory work related to NAV calculation errors.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
3.1	Responsive supervision of proposed and implemented **changes in firms operating processes and arrangements**, with a focus on capacity to respond effectively to **stresses in market conditions**.	●	●	●	●
3.2	Deeper dive into the appropriateness of industry approaches and processes for **monitoring investment restrictions** and **reporting regulatory breaches**.		●	●	●
3.3	**Value at Risk (VaR) model review** with a focus on UCITS that opt to the use of the VaR approach and the effectiveness of the **levels of oversight by depositaries.**	●	●		
3.4	Continued **enhancement and use of fund data and risk models** by the Central Bank to deliver a data-led, agile and risk-based approach to the effective and efficient oversight of the funds sector.	●	●	●	●
3.5	Review of **valuation oversight** with a focus on **hard to value assets** and the **oversight role of the depositary.**	●	●		

Focus Area 4: Liquidity and leverage risks

Pockets of vulnerability persist where funds have higher leverage or liquidity transformation, or both. Swift shifts in sentiment can lead to "dashes for cash", elevate margin and collateral calls and put pressure on dealing arrangements. Money market funds (including public debt constant NAV and low volatility NAV structures) can face acute liquidity strains given intraday dealing and investor expectations of par value. These dynamics matter for investor protection, particularly where liquidity management tools may restrict access, and for financial stability given the potential for fire sale dynamics and spillovers.

Back to "Contents"

Our expectation is that firms maintain robust, documented leverage and liquidity risk management frameworks proportionate to their risk profile. Firms need to align redemption frequency, notice and settlement periods with portfolio liquidity under normal and reasonably foreseeable stressed conditions. Appropriate liquidity management tools need to be selected and operated, supported by effective governance, stress testing (including margin and collateral scenarios) and contingency plans. Funds with higher leverage or structural liquidity mismatches - including certain liability driven investment (LDI) strategies and vehicles investing in less liquid assets - should be able to demonstrate enhanced controls, clear escalation pathways and operational readiness to deploy liquidity management tools when warranted.

We will continue to focus on liquidity risk management, including through communication of the Central Bank's recent work on liquidity management tools as well as a thematic review on cohorts identified by our fund risk model as engaging in significant liquidity transformation. Our initial focus will be on selected Irish authorised bond funds and managers. In parallel, under Article 25 of the Alternative Investment Fund Managers Directive (AIFMD), we will analyse leverage-related systemic risks across funds and cohorts, identify the most leveraged alternative investment funds and undertake targeted reviews of those funds and their Irish AIFMs, including where Irish AIFMs oversee non-Irish funds. This will involve examining liquidity risk management, stress testing and contingency arrangements. We will continue our supervision of Irish authorised property and LDI funds within their respective macroprudential frameworks and engage with firms where vulnerabilities are identified.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
4.1	Review on **liquidity risk management in bond funds** to assess how firms manage the mismatch between investor redemptions and asset liquidity.	●	●	●	●
4.2	Review the progress of relevant **AIFMs on leverage reduction and maintenance plans across property funds**.	●	●	●	●

Back to "Contents"

		H1 26	H2 26	H1 27	H2 27
	Property funds questionnaire issued in Q1. Submission of return, assessment of responses and follow up engagement through H2 2026.	●	●	●	●

Focus Area 5: Product costs and disclosures

An investor-centric culture is essential to protect consumer and investor interests, and to mitigate the risk of funds or firms failing to identify, escalate or remediate issues that could cause harm, particularly to retail and vulnerable clients. We have noted a continued increase in engagement by funds and FSPs in relation to proposals for investment in complex and innovative investment strategies and alternative assets including crypto-assets, private debt and novel exchange traded fund (ETF) constructions. Another key area of innovation relates to tokenisation. This has the potential to introduce efficiencies and broaden access to investment products for investors. We have noted strong levels of engagement with organisations working on tokenised proposals with live applications under review.

Given the risks connected to these instruments combined with the growth in digital retail platforms, it is important that funds and FSPs adequately consider their unique features, their transparency and their suitability for the fund's target market. Retail investors need to fully understand the nature of the investment objectives, associated risk profile and the characteristics of specific asset classes before investing.

Through our robust gatekeeping process, we will continue to constructively engage with industry in relation to the potential to establish funds that give exposure to instruments which have previously been considered as presenting comparatively higher risk. This allows the Central Bank to consider the appropriateness of different types of instruments in portfolios targeting different segments of the market. Investment product strategy and suitability require robust governance to prevent the marketing of inappropriate products to non-professional investors. Firms must ensure product design, target market assessment and distribution practices align with investor needs and risk tolerances.

Back to "Contents"

With a view to protecting the best interests of investors, costs and fees charged to investors must be clearly justified and transparent. Fee models should be calibrated proportionately to reflect the services provided and the associated costs. There should be strong governance and oversight by the FMC to reflect this. Clear, comprehensive disclosure of fees as well as full transparency of all underlying costs are necessary to avoid undue charges and ensure investors are fully informed.

Aligned with the EU picture more broadly, the level of direct retail participation in Ireland is quite low. This limits households' ability to benefit from potentially higher long-term returns aligned to their risk appetite and tolerance. There are several barriers at play, including accessibility, levels of understanding, taxation and overall levels of confidence. The Irish funds sector has a significant part to play in providing good quality, understandable products to retail investors that meet their needs, delivering on the core elements of the Savings and Investment Union agenda.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
5.1	Continued engagement both domestically with regulated firms in the funds sector and internationally with ESMA on **costs and fees with a focus on value for money**. Ongoing supervisory engagement where breaches relating to **inappropriate cost/fee structures** or **disclosures** have been identified.	●	●	●	●
5.2	**Gatekeeping**, which is a vital tool for the Central Bank regarding assessing fund disclosures, levels of costs and transparency for prospective investors.	●	●	●	●
5.3	Consistent application of the principles of the **Consumer Protection Code**, assessing how firms are implementing it.	●	●	●	●

Focus Area 6: Data and artificial intelligence

Whilst there continues to be improvements in data quality across the funds sector, the risk remains that poor data quality, accuracy and reliability can undermine effective governance and decision-making within firms and our ability to supervise. Without robust

Back to "Contents"

validation and reconciliation of data sets, particularly where this data drives AI system generated actions and decisions, there is a heightened risk that strategic, financial or operational actions will be based on incomplete data, potentially leading to poor outcomes for both the firm and its investors. This was evident in our most recent sectoral review of delegation where we observed significant gaps at some FMCs in data accessibility, contingency planning for data loss or interruption and in governance of data.

The growing deployment of AI across the funds sector brings its own set of risks when awareness, governance and controls are inadequate. While AI systems can enhance portfolio managers' efficiency, higher levels of autonomy and adaptive learning increase the complexity of trading activity, potentially resulting in disorderly market behaviour, unfair investor outcomes or even market manipulation. The growing reliance on third-party AI service providers further compounds oversight and data management challenges. Where firms are utilising these services, they must have appropriate governance and controls frameworks in place to mitigate against the relevant risks.

As firms increasingly rely on sophisticated quantitative models for stress testing, scenario analysis and statistical assessments, the potential for errors in model design, calibration or implementation rises. This could amplify the chance of unintended market impacts or manipulative practices. Rigorous model governance - including thorough validation, ongoing performance monitoring and strong documentation - is essential to mitigate these risks across the funds sector.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
6.1	Continued enhancement and use by the Central Bank of **fund data and risk models** to deliver a data-led, agile and risk-based approach to the effective and efficient oversight of the funds sector.	●	●	●	●
6.2	Continued engagement to understand **firms' approach to and usage of AI** in their business models.	●	●	●	●

Back to "Contents"

Focus Area 7: Climate and ESG-related risks

The Central Bank's approach to supervising climate and ESG risk spans both the authorisation and ongoing supervisory engagement processes. It works to ensure that regulated firms in the funds sector are robustly integrating and managing these risks in line with regulatory expectations and protecting investors. We continue to focus on driving high standards for ESG funds, addressing greenwashing risk and assessing climate risk as the regulatory landscape and investor demand for ESG products advances. We have adopted a data driven approach to supervising these risks with a bespoke ESG dashboard in place allowing us to use advanced natural language processing techniques to analyse large volumes of ESG data, assess portfolio level data and compliance with the Sustainable Finance Disclosure Regulation (SFDR).

We continue to see a level of regulatory divergence across the theme of ESG which can impact the consistent application of sustainability standards and market conduct across markets. This can result in the reduction of investor confidence and limit comparability across markets. However, initiatives such as the Fund Naming Guidelines and further engagement at a European level focused on the application of SFDR should provide for a more consistent approach. Any revisions expected through the implementation of SFDR 2.0 will also be an area of focus for supervisors as we progress to this updated regime.

The Central Bank recently published an industry report outlining our supervisory findings and expectations from the ESMA CSA on sustainability and disclosure risk.[52] The report highlighted that firms are making progress in embedding SFDR requirements, however, there are areas for improvement including inconsistent sustainability risk monitoring, data quality challenges and unclear product disclosures. The report emphasises firms' responsibility to maintain robust controls, ensure transparent disclosures, and stay aligned with evolving regulatory guidance to prevent greenwashing and support investor decision-making aligned with sustainability preferences.

The main planned activities relating to this supervisory focus area are:

[52] See the Central Bank of Ireland (October 2025), *ESMA Common Supervisory Action on Sustainability Risks and Disclosures in the Investment Funds Sector*.

Back to "Contents"

		H1 26	H2 26	H1 27	H2 27
7.1	Sustainability work will continue using the Central Bank's **ESG dashboard tool** to assess firms' **compliance with SFDR**.	●	●	●	●
7.2	**Compliance with the Fund Naming Guidelines** will continue to be monitored at both the gate and through data-led supervisory reviews.	●	●		

Back to "Contents"

Markets Sector

KEY TAKEAWAYS

- Securities markets are exposed to increased uncertainty and geopolitical risk in the global macro environment leading to more frequent episodes of market volatility and shifts in trading volumes across all asset classes. Primary issuance in crypto securities is growing, debt issuance remains robust, but equity issuance continues to decline due to structural issues.
- Trading firms and venues continue to generate healthy profitability and capital buffers, but their heavy technology dependency and growing reliance on outsourced providers raises the probability and potential impact of outages and cyber incidents.
- Crypto Asset Service Providers (CASPs) are a new category of regulated entity within the markets sector. CASPs introduce elevated consumer protection, client asset safeguarding and financial crime risks that are distinct from traditional trading firms and venues. CASPs' larger retail client bases, novel custody models and complex market structures result in unique supervisory considerations and priorities.

Sector profile

- The sector includes regulated firms and regulated activities by issuers and individuals engaging in capital markets activities. It operates under a large and complex regulatory framework. It comprises the Irish Stock Exchange, trading venues, proprietary/trading firms (market makers, systematic internalisers) and CASPs. Many firms are part of large international groups and undertake significant business activities in other countries.
- The Irish Stock Exchange is critical for the primary market regarding listing in Ireland (while for debt listing activity it has global scale) and secondary market for trading in Irish equities.
- Trading firms and venues are wholesale, technology intensive and provide liquidity and price formation across asset classes. There are eight trading firms authorised, including four of the most significant market makers in EU securities markets. There are five trading venue operators authorised, including the Irish Stock

Back to "Contents"

Exchange and one of the most significant dark trading venues in the EU.

- CASPs provide trading, custody, brokerage and portfolio services and have a higher retail client presence than traditional market firms. CASPs create different risk profiles, particularly on custody of crypto assets, AML/CFT and consumer outcomes. Ten CASPs were authorised in 2025 with a mix of retail-focused and institutional-focused business models.
- In 2025, the Central Bank approved 649 prospectus documents, received 20,823 filings of Final Terms and received 305 crypto asset whitepaper notifications.

Our supervisory approach to the sector

Firms are supervised on a sectoral basis, except for one supervised on a close and continuous basis. It is our objective that the regulatory and supervisory environment enables the potential benefits of innovation for consumers, businesses and society to be realised, while ensuring that the risks are effectively managed and mitigated.

Our supervisory activities will focus on a mix of direct engagement and sectoral thematic reviews and, specifically for MiFID firms, proactive supervisory review and evaluation cycles.[53] These activities cover key areas such as firms' operational resilience, market abuse surveillance, conflicts of interest approach, liquidity and capital adequacy. Reactive supervision is undertaken based on the review and monitoring of regulatory and financial returns, including based on trigger events and indicators.

We highlighted financial resilience as a key focus area in last year's RSO, specifically in relation to the impact of volatility on market risks. Assessments to date conclude that firms have generally been profitable with sound capital and liquidity buffers in place. Much of our ongoing assessments will be less extensive in 2026. Recent assessments have also identified that the approach to risk management and internal capital planning across the sector requires a more mature approach to capital risk management and this will be a focus in 2026 engagements. Notwithstanding current buffers, it is

[53] For detailed information on the supervisory review and evaluation process (SREP) under the Investment Firm Directive, see *Supervisory Review Process*, Central Bank of Ireland website.

Back to "Contents"

important that firms continue to maintain their financial resilience given the volatile and uncertain operating environment.

Work is well underway to embed an appropriate supervisory approach for the recently established CASP sector. For 2026, there will be a focus on reactive supervision as the newly authorised CASPs seek to deploy their business models. In Q1, we will launch a new quarterly CASP regulatory return, which will provide us with a detailed view of each CASP's financial position and will inform our supervisory engagement.

We continue to focus on improved transparency around climate change and ESG disclosure. With the implementation of the Listing Act - a package of legislative measures aimed at simplifying disclosure requirements and listing rules for companies issuing securities or listing on public markets, including ESG disclosures - throughout H1 we will carry out workshops with industry and additional engagements to ensure industry preparedness.

Sectoral assessment and supervisory focus areas

Focus Area 1: Operational and cyber resilience

Operational resilience is the markets sector's most pervasive risk and has increased in priority for supervisors in 2026. To serve the interests of consumers, investors and issuers, markets must remain open and accessible in an increasingly uncertain and volatile world. A market that is closed or suffers frequent unavailability, is one that undermines the interests of investors, stability and the real economy. The combination of the centralisation of digital processes, rapidly evolving and heavy reliance on technology, increased reliance on the cloud, the major role of a small number of third-party providers, and the threat landscape makes it a critical concern for this sector.

Market firms have strengthened their baseline operational resilience and incident reporting, but the level of maturity remains uneven across the sector. Shared reliance on a small number of vendors creates concentration risk and approaches to stress testing and contingency planning vary widely. Additionally, in our deep dives during authorisation assessments, we observed that CASP business models introduce distinct technical challenges, including the security of private keys. These add a further layer of operational and consumer risk. The core supervisory objective is that firms meet their obligations under DORA and have robust operational resilience frameworks in place. This is so that, when faced with disruption,

Back to "Contents"

uncertainty or shocks, they can maintain the critical and important services they provide to the market and its participants.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
1.1	**Operational resilience assessments** contribute materially to the **SREP process for MiFID firms** as part of internal governance & controls risk review. We will conduct sector-wide reviews and hold firm-specific engagements on: – Technology risk and resilience – Operational resilience maturity – Market outages – DORA compliance	●	●		
1.2	Targeted work will be conducted on **CASPs** in relation to **DORA compliance**, in line with authorisation conditions.	●	●		
1.3	Thematic review to be undertaken by **ESMA** in respect of **cyber risk** as part of a wider **Common Supervisory Action** (CSA) on the newly established CASP sector.		●	●	●

Focus Area 2: Treatment of customers

The volatile and inherently high-risk nature of crypto leads to a significant risk for consumers and investors. The features of crypto and the complex business models of CASPs, including the sophisticated products offered, lead to a heightened risk of consumer and investor detriment. Poor or opaque disclosures and product unsuitability can lead to decisions by customers that may cause them harm. Business models and product offerings are evolving with the emergence of new services that introduce additional complexity, for example, copy trading, automated portfolio management or code free trading.

We expect firms to have strong governance and risk management frameworks in place, including clear disclosures to their customers, and the provision of suitable products and marketing to their customers in a transparent and consumer centric manner. Firms are

Back to "Contents"

expected to engage with us before making material changes to their business including new products or services. For this new sector, reinforcing and being clear on our expectations is critical, as such we will continue to be explicit in our public communication and industry engagement.

Notification of MiCAR Title II Whitepapers are a new area of responsibility for the Central Bank with the regime being effective since January 2025. In accordance with the MiCAR framework, the Central Bank is responsible for receiving notifications of whitepapers for these crypto assets instruments and assessing that the relevant disclosures are appropriate.[54] Over 300 Title II whitepapers were notified to us in 2025, with volumes exceeding predicted levels.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26
2.1	Build awareness and set out the Central Bank's expectations through ongoing **industry engagement**, including at our **annual CASP event** where we will outline our supervisory priorities.	●	●
2.2	**White papers:** Given the increasing risks associated with the rapid transformation of the crypto-asset sector and the increasing numbers of whitepapers the Central Bank is receiving, we will fully engage in the **ESMA work on MiCA regulation**.	●	●

Focus Area 3: Custody of crypto-assets

The service of custody and administration of clients' crypto-assets involves the safekeeping or controlling of clients' crypto-assets, or the means of access to those assets which is typically in the form of private cryptographic keys. Given the digital nature of crypto-assets, custody in this sector presents a heightened risks of loss or theft (including the risk of hacking), or mismanagement (including poor cyber-risk management or ineffective related governance and controls). There is a risk that an absence of robust governance and controls over client crypto-assets arrangements results in the loss,

[54] MiCAR Title II Whitepapers are legally mandatory, comprehensive information documents that issuers must publish before offering "other" crypto-assets (excluding asset-referenced or e-money tokens) to the public or seeking trading admission in the EU. They are designed to achieve transparency, providing fair, clear, and non-misleading information regarding the project, issuer, risks, rights, and technology.

Back to "Contents"

misuse or misappropriation of clients' crypto-assets, or delays in their return in the event of firm failure.

MiCAR sets clear requirements for authorised CASPs when providing custody and administration of clients' crypto assets. Since last year's RSO, there have been a number of CASPs authorised in Ireland to provide the service of custody and administration of crypto assets. We expect CASPs to continually reassess the appropriateness of their custodial arrangements to ensure they remain fit for purpose particularly where the nature, scale or complexity of their operations changes. As part of our robust assessment of CASPs' arrangements at authorisation, when deficiencies were identified we communicated our clear expectations to the firms regarding client assets safeguarding. Where we applied authorisation conditions, we will be following up with the affected CASPs to ensure their implementation during 2026.

The main planned activity relating to this supervisory focus area are:

		H1 26	H2 26
3.1	Follow-up work to examine CASPs' **compliance with the custody requirements outlined in MiCAR** and related authorisation conditions.		●

Focus Area 4: Financial integrity

The pseudonymous and cross border nature of crypto flows increases the risk of money laundering and terrorist financing activities. The opaque nature of the market structures in the crypto asset sector can make detection and tracing of these activities difficult. Due to limited sector experience of evolving typologies, their fast onboarding, complex cross border flows and fragmented know you customer and transaction monitoring, AML/CFT remains a key supervisory focus. We expect CASPs to maintain effective AML and fraud-prevention controls to mitigate financial crime risks in this rapidly evolving sector.

The main planned activities relating to this supervisory focus area are:

Back to "Contents"

		H1 26	H2 26
4.1	**Trading firms and CASPs** will be required to complete an **enhanced Risk Evaluation Questionnaire (REQ)**. The enhanced REQ will capture detailed quantitative and qualitative risk information on ML/TF risk and the quality of AML/CFT controls. This data will be used to: (a) identify firm and sector-specific issues and emerging trends; (b) guide supervisory strategy; and (c) satisfy incoming data requirements for AMLA. Following completion by Trading Firms and CASPs of the AML REQ in H1, we will carry out work across the sector to develop the AML risk profile for the relevant entities.		●
4.2	**Targeted assessment of certain CASPs**, which will include on-site engagement to ensure that **AML controls and processes** are effective.	●	●

Focus Area 5: Market abuse and market surveillance

Market integrity depends on effective surveillance by market firms and regulators across traditional and crypto trading environments. Surveillance effectiveness underpins confidence and transparency in price formation and acts as a deterrent to abusive practices. Suspicious Transaction Order Reports (STORs) and wider Market Abuse Regulation (MAR) reporting and disclosures along with the Central Bank's own surveillance framework are fundamental to achieving market integrity and the confidence in the market that comes with it.

Through last year's SREPs and onsite reviews, we have observed that some firms in the sector are implementing new approaches to the management of market abuse risk and surveillance, including implementing new trade surveillance systems. Crypto markets pose additional detection challenges over and above traditional assets due to their borderless nature, pseudonymity and novel complexities surrounding the structure and mechanics of distributed ledger technology (DLT). Success is characterised by improvements in the timeliness of delivery of high-quality STOR submissions with effective follow up actions by firms, effective surveillance management information to preapproved control function holders and boards, and a demonstrable increase in detected abuse. These would demonstrate a valuable element of self-policing by the market.

Back to "Contents"

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26
5.1	**Review of venue and firm trade surveillance implementations and frameworks,** work with industry to improve **STOR** submission and quality, enhance our existing surveillance program in traditional asset classes, and work with NCAs to coordinate surveillance capability improvements for crypto markets within the EU.	●	●
5.2	Cross-sectoral thematic review of **market abuse frameworks and surveillance.**	●	●
5.3	Targeted inspections on **compliance with Market Abuse Regulation (MAR) requirements** for persons discharging managerial responsibilities.		●

Focus Area 6: Conflicts of interest and controls

Poorly managed conflicts of interest have the potential to cause harm to investor and consumer interests and present a broader risk to market integrity. Ineffective structural and governance arrangements within firms can create a culture which dilutes the importance of prevention and may even facilitate conflicts. Weaknesses in control frameworks may result in ineffective or incomplete detection, escalation and management of market conduct risks including unauthorised or disorderly trading.

While some conflicts are inherent in some business models, firms are required to identify and mange conflicts. We expect that firms take all reasonable steps to ensure there are appropriate controls in place to give investors and consumers sufficient protection from market conduct risks. The Central Bank will continue to have direct engagement with firms in relation to their conflicts of interest framework and their management and prevention of associated risks.

The main planned activities relating to this supervisory focus area are:

Back to “Contents”

		H1 26	H2 26	H1 27	H2 27
6.1	Build on the 2025 SREP work in this area and continue to examine firms' **governance structures and the controls** in place to ensure **conflicts of interests** are prevented and managed to protect the interests of investors, consumers and market stability.	●	●		
6.2	Cross-sectoral thematic review of **conflicts of interest management in wholesale firms.**	●	●		
6.3	Cross-sectoral thematic review of **unauthorised trading and trading controls.**		●	●	●

Focus Area 7: Artificial intelligence

The use of AI in trading and market making is not a new phenomenon, with firms having deployed AI models to different degrees and with varying levels of model governance and board awareness around its use. Increasingly firms in the sector are building on legacy algorithmic approaches with a focus on generative AI use in secondary markets. Use cases range from price prediction models, trade surveillance and cyber security.

Following our engagement with the sector last year on the use of AI by wholesale market participants, governance and explainability are central supervisory concerns. While there has been an increase in the use of advanced AI tools in the trading lifecycle within market firms, gaps exist in relation to technical expertise at the local level to explain the complex technologies. There appears to be significant reliance on group expertise and governance structures in the development and application of AI, and in the setting of the control environment at local level.

Unchecked AI deployment can amplify market instability or introduce opaque decision making that complicates accountability. Transparency and explainability risks create challenges for firms to identify, manage and mitigate risks arising from the use of AI. In addition, firms should be aware of risks relating to the misappropriation of information using deepfakes. Success is evidenced through clearly reviewed and documented governance, explainable systems, accountability for decisions, oversight and appropriate human in the loop controls.

Back to "Contents"

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26
7.1	We will build on work already completed to collect sectoral AI intelligence and conduct **targeted inspections where AI materially affects trading or surveillance**.	●	●
7.2	We will integrate **governance reviews** into **SREP assessments of MiFID authorised firms**.	●	●

Back to "Contents"

MiFID Investment Firm Sector

KEY TAKEAWAYS

- Operational resilience has increased in priority for supervisors. Operational and cyber disruptions are now high probability events. The ability of firms to identify, respond to, recover and learn from such events remains an increasingly challenging topic. Firms must ensure that their operational resilience frameworks are robust and commensurate with the nature, scale and complexity of their business.
- Firms' treatment of investors is another key focus area. We want to see that investor interests are at the heart of the culture, strategy and business model of the firm. We expect firms to prioritise the application and embedding of the relevant aspects of the revised Consumer Protection Code guidance into their business.
- The sector provides an important gateway for investors to access financial products and services. Consumers should have appropriate levels of availability and choice and be empowered to make effective decisions to meet their financial needs.
- We will work closely with our European colleagues to support ESMA's supervisory convergence work given the cross-border nature of the provision of investment services. We will also support the evolution and implementation of key EU initiatives including the Retail Investment Strategy.

Sector profile

- The sector is diverse in the nature of products and services provided and the size and scale of firms. It includes wealth and portfolio managers and online broker platforms, as well as firms providing pension-related services and engaging in capital market activity.
- 80 firms are authorised in Ireland with a further 11 firms authorised in other EU member states operating in Ireland on a freedom of establishment basis via a branch or tied agent.
- Firms in the sector provide a variety of investment products and services to more than a million retail investors and 50,000 professional investors across Europe, providing both advisory and non-advisory services.
- There continues to be a robust pipeline of new applicant firms as well as existing firms seeking additional permissions to support

Back to "Contents"

business expansion. The authorisation assessment is rigorous and proportionate, reflecting the nature, scale and complexity of applicant firms' activities.

Our supervisory approach to the sector

There will be a continuing focus on assessing the effectiveness of governance and risk management arrangements, and culture and "tone from the top" in firms. We continue to see variances in the maturity of governance and risk management frameworks and culture on display in firms across the sector. A particular focus will be placed on board accountability and how firms have embedded their responsibilities under the IAF/SEAR and how they are putting investors' interests at the heart of their business.

We will remain focused on supervisory review and evaluation process (SREP) assessments. A targeted review of the business models of a cohort of SREP category 2 firms will commence in Q2 2026. In addition, a significant portion of our supervisory work is driven by day-to-day sectoral supervision matters ranging from analysis of regulatory and financial returns to assessing PCF applications.

In addition to the five supervisory focus areas outlined below, we will continue to address the topics highlighted in the 2025 RSO, such as financial resilience and the safeguarding of client assets. The outcome of our supervisory activities and firms' own work in these areas has resulted in the sector being more financially resilient, with firms having sound capital and liquidity buffers in place and robust client asset safeguarding arrangements. Nonetheless, it is important that firms are not complacent and continue to maintain their financial resilience, given the volatile and uncertain operating environment, and to ensure their client asset arrangements remain fit for purpose.

Sectoral assessment and supervisory focus areas

Focus Area 1: Operational and cyber resilience

An operationally resilient firm can recover its critical or important business services from a significant unplanned disruption, while minimising the impact on its investors and the wider financial system. When an operational disruption occurs, including a cyber incident, this can result in investors losing access to their account, incurring a financial loss or having their personal data compromised.

Back to "Contents"

Enhancing operational resilience across all sectors is a strategic priority for the Central Bank and will help build investor trust and confidence in their dealings with firms.

A recent thematic assessment found a maturing of operational resilience frameworks across the sector, however there were varying degrees of maturity seen in the sample of firms covered. [55] Rising cyber threats, coupled with the concentrated reliance on a relatively small number of third-party ICT providers, increase the risks of technological disruption. We expect all firms to act on our assessment findings and build on their existing operational resilience foundations. They should ensure they are sufficiently resilient from a cyber and digital perspective to withstand future disruptions or incidents. Firms' leadership should ensure that resilience is embedded into their strategic decisions and boards should prioritise activities and target investment that make critical or important business services more resilient.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
1.1	Engagement and risk assessments across **certain SREP category 1 & 2 firms**. This will include continued engagement in response to findings from thematic work conducted in 2025 and targeted engagement with certain firms in relation to the **establishment and maturity of operational resilience frameworks** in accordance with the Central Bank's cross industry guidance.	●	●	●	●
1.2	Engagement with **certain SREP category 1 & 2 firms** in relation to **IT risk management frameworks**, **DORA implementation** and **cyber resilience**. This will include the issuance and assessment of firms' self-assessment by way of the Central Bank's IT risk questionnaire.	●	●	●	●
1.3	Supervisory assessment of **DORA** incident reporting and registers of information annual submission.	●	●	●	●

[55] See Central Bank of Ireland (December 2025), *Thematic Assessment: Operational Resilience in the MiFID Investment Firm Sector*.

Back to "Contents"

Focus Area 2: Conflicts of interest

In last year's RSO, we highlighted that firms were demonstrating a lack of understanding of how conflicts of interest can hamper their delivery of positive investor outcomes. We continue to see this and expect firms to place sufficient focus on the identification and management of conflicts of interest within their business activities. Firms must continually evaluate their inducement and remuneration policies to ensure they drive the right behaviours and standards, thus building investor trust and supporting greater participation in capital markets by individuals. Firms must secure investors' interests and effectively manage any conflicts of interests by placing investors at the heart of their decision making.

Risks continue to exist for investors where firms providing investment services have an incentivised remuneration model. Inducements, commission and remuneration structures can lead to an inherent conflict of interest between revenue generation and acting in the best interests of clients. A lack of understanding of these conflicts of interest and the implications in terms of value-for-money for investors can lead to poor outcomes for investors.

This is a key focus area for ESMA who recently announced a Common Supervisory Action (CSA) on conflicts of interest in the distribution of financial instruments.[56] The CSA will assess how firms comply with their obligations to identify, prevent and manage conflicts of interests when offering investment products to retail investors, with a particular focus on remuneration and inducements. The CSA will also consider the role of digital platforms in directing investors towards certain products, and whether this serves their best interests. In addition, we will undertake a thematic review to evaluate firms' awareness of conflicts of interest within wholesale business models.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27
2. 1	Participation in the **ESMA CSA on conflicts of interest** in the distribution of financial instruments. In line with the prescribed ESMA methodology, a sample of firms providing investment	●	●	

[56] ESMA (December 2025), *ESMA to launch Common Supervisory Action on MiFID II conflicts of interest requirements*.

Back to "Contents"

		H1 26	H2 26	H1 27
	advice and firms offering non-advisory services will be selected for inclusion in the scope of this CSA.			
2.2	Firm specific feedback and an industry communication on the **findings of the CSA work** and our supervisory expectations.			●

Focus Area 3: Treatment of investors

The implementation of the revised Consumer Protection Code should be a priority item for all firms. While the Code does not apply in its entirety to this sector, firms will need to embed the guidance on securing customer interests and the protection of consumers in vulnerable circumstances aspects into their operations. Ensuring firms are embedding the guidance supporting the revised Code will be an ongoing area of focus for us. Vulnerable investors will require additional protection and support when engaging with firms. It is, therefore, important that firms understand vulnerability and the ways in which investors in certain circumstances can be vulnerable.

The sector provides an important gateway for retail investors to access financial products and services. In line with the EU more broadly, the level of direct retail participation in Ireland is quite low. The sector has a key part to play in building trust and confidence, including through providing understandable information and good quality financial products and advice to (potential) investors.

Digitalisation brings many benefits including ease of access for investors, with the increasing use of online and digital platforms and social media being evident. There is a risk to investors from inappropriate marketing and advertising practices, however, which is amplified by the move away from traditional means of marketing and advertising. All marketing and advertising content should be fair, clear and not misleading and presented in a manner that seeks to effectively inform investors.

There is a heightened risk that unsuitable products are held or chosen by investors, particularly retail investors, where ineffective product governance frameworks are in place. Firms may fail to identify the target market for products at a sufficiently granular level and there may be insufficient oversight and challenge of product offerings by senior management. We expect firms to offer products

Back to “Contents”

clearly aligned to investors' changing goals, risk capacity and preferences, delivering fair value and ongoing suitability.

The increase in the number of complaints from investors is a continuing trend. We expect firms to be able to demonstrate robust complaint handling processes. Prompt identification of potential complaints and their timely resolution can prevent an issue becoming more significant leading to a better outcome for both the investor and the firm itself. Monitoring and analysis of complaints management information, identifying root causes and taking action to address them, can prevent future issues arising, thereby helping to secure the interests of all investors, not just those raising the complaints.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
3.1	Cross-sectoral thematic review on the identification and treatment of **customers in vulnerable circumstances.**		●	●	●
3.2	A thematic review of **complaints handling** began in Q4 2025. The review will consider how firms deal with individual customer complaints and use MI to identify trends and mitigate against recurring issues.	●	●		
3.3	The **ESMA CSA on conflicts of interest** in the distribution of financial instruments will include a focus on **digital/online platforms**.	●	●	●	
3.4	The new Code and related guidance will be embedded into supervisory practices and firm engagements.	●	●	●	●
3.5	We will deploy an **enhanced Conduct of Business return** to support our data driven approach to supervision.			●	●

Focus Area 4: Artificial intelligence

The use of AI in investment services can bring efficiencies and new capabilities, but it also raises material risks to investors and to market integrity if not deployed in a manner that has regard to investors' interests. Increasing autonomy and adaptiveness in AI can produce complex, multi-layered behaviour that is hard to explain or

Back to "Contents"

constrain, increasing the risk of unfair or inequitable investor outcomes, incorrect or biased advice, and even market manipulation. Poorly governed AI - including models that are mis-specified, inadequately tested, or deployed without attention to explainability, data quality and privacy - can harm investors, erode trust and threaten the stability and integrity of markets.

Firms are expected to treat AI like any other material technology risk by adopting robust governance, risk management and compliance frameworks. Ensuring model validation, ongoing monitoring, testing and incident readiness is essential. AI adoption should be aligned with a firm's strategy and risk appetite, with ethical data practices and privacy safeguards adopted.

MiFID II requirements are technology-neutral and firms remain responsible for discharging all their obligations when relying on AI technologies in the provision of investment services. To gain further insights into use cases, over the course of 2026 we will assess firms' use and application of AI in the provision of services, with a focus on digital interfaces.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
4.1	Engagement with firms to continue to develop our **understanding and assessment of AI use cases** in the sector to inform our supervisory approach and expectations of firms. We will bring an AI focus to all our thematic reviews.	●	●	●	●
4.2	Support any future work and surveys undertaken by **ESMA** on AI, including further analysis of the 2025 survey results.	●	●	●	●

Focus Area 5: Financial crime

MiFID firms provide access to the financial system for a broad range of clients and counterparties on a domestic and pan-European basis, making them an attractive target for criminals. Furthermore, as highlighted in the 2025 RSO, the diverse customer base and cross-jurisdictional ownership structures can increase the risk of money laundering. Supervisory engagements and regulatory returns from firms indicate that control weaknesses exist across the sector. Inadequate AML/CFT controls create an increased risk that

Back to "Contents"

the financial system will be misused for money laundering and terrorist financing, weakening the integrity of the Irish financial system.

Firms must fully understand and continuously assess the ML/TF risks specific to their business models, adapting swiftly to emerging threats and evolving typologies. Boards and senior management are reminded that they must be able to demonstrate an understanding of their firms' key ML/TF risks and the adequacy of their AML/CFT risk management and control frameworks in line with national and European requirements (including AMLA). Firms are expected to implement a proactive, outcome-driven approach that goes beyond compliance, protecting the integrity of Ireland's financial system and fostering investor trust and confidence.

The nature of frauds and scams is evolving rapidly leading to the risk that firms have inadequate systems and controls in place to protect their investors from such criminal activity. Their controls must also protect clients' personal data from loss or misuse. We expect firms to be vigilant and to have robust controls in place to reduce the likelihood of frauds and scams occurring and to demonstrate fair outcomes for investors who fall victim.

STOR submissions from the sector have increased in volume and we have seen an improvement in their quality, however, concerns remain. Failures by firms to implement effective, proportionate market surveillance systems and procedures to detect and assess possible market manipulation or insider trading risk allowing abusive behaviour by market participants to go undetected and unreported. This, in turn, undermines the integrity and proper functioning of the financial system. In addition, ineffective control frameworks may fail to identify or prevent unauthorised or disorderly trading. Potential failures in pre or post trade controls risk erroneous trades causing financial loss and increased market volatility.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
5.1	Firms with **higher impact ML/TF ratings** are subject to **cyclical reviews**, such firms may be subject to inspection and/or review meetings during the year.	●	●	●	●

Back to "Contents"

		H1 26	H2 26	H1 27	H2 27
5.2	Firms will be required to complete an **enhanced Risk Evaluation Questionnaire (REQ)** which will capture detailed quantitative and qualitative risk information on ML/TF risk and the quality of AML/CFT controls. This data will be used to: (a) identify firm and sector-specific issues and emerging trends; (b) guide supervisory strategy; and (c) satisfy incoming data requirements for the EU's Anti-Money Laundering Authority (AMLA).	●	●	●	●
5.3	Reviews of **venue and firm trade surveillance** implementations and frameworks, working with industry to **improve STOR submission** and quality, enhance our existing **surveillance program**.	●	●	●	●
5.4	Thematic review of a **sample of MiFID investment firms** to be included in a **market abuse frameworks and surveillance thematic review** alongside other sectors.	●	●		

Back to “Contents”

Retail Intermediaries Sector

KEY TAKEAWAYS

- The retail intermediaries sector plays an important role in the Irish financial services market. It is a key distribution channel for insurance, pensions, investments and mortgage products.
- With their client-facing role, retail intermediaries should focus on securing their customers' interests and delivering positive outcomes by ensuring that consumers are at the heart of their culture, strategy and business model.
- It is important that all retail intermediaries have plans in place to recover from material operational disruptions and to support consumers during any incidents. The plans should be commensurate with the size, scale and complexity of their business.
- Unregulated activity is a key area of focus for the Central Bank. Where products are outside the scope of regulation, consumers do not benefit from the protections afforded by the regulatory regime. Under the revised Consumer Protection Code, there is a greater delineation between regulated and unregulated products or services with firms required to use clear distinctions in terms of branding for their regulated and unregulated entities.
- Mergers and acquisitions continue to be observed in the sector. We will conduct a review of this activity to gauge the overall impacts on the market and consumers, and to inform supervisory strategy.

Sector profile

- Retail intermediaries provide a gateway to investments and capital markets, but current levels of retail investor participation are low. Retail intermediaries have an important role to play in building the trust and confidence that underpins greater retail investment participation.
- Diverse, with some 2,500 authorised retail intermediaries at the end of 2025, with firms across every county in Ireland. This comprises insurance intermediaries, investment intermediaries and mortgage intermediaries. Many intermediaries hold more than one licence.

Back to "Contents"

- Majority of firms (c 89%) are small and have less than 5,000 clients, while some larger and more complex firms have hundreds of thousands of clients.
- The sector also includes debt management firms and crowdfunding service providers. Most of those availing of crowdfunding services are retail investors.

Our supervisory approach to the sector

Our supervisory activities and interventions are undertaken on a sectoral and cross-sectoral basis, with firm specific engagement where appropriate. Planned activities are set out below and cover five focus areas with a particular focus on securing customers' interests. There will be continued robust assessment of authorisation and fitness and probity applications.

We will continue to rely on the analysis of regulatory returns and our market intelligence to identify risks and trends. If any concerns are prompted, or actual adverse situations or risks come to our attention from any source, the issues will be triaged and investigated with appropriate and proportionate actions taken.

We recognise the importance of regular and open sectoral communication and engagement with the sector. This will continue to be a focus in 2026 enabling us to listen to practitioners, deliver our key messages, clearly set out our supervisory expectations and remind firms of their obligations.

Sectoral assessment and supervisory focus areas

Focus Area 1: Operational and cyber resilience

Financial service providers, including retail intermediaries and crowdfunding service providers, place significant reliance upon technology to deliver services to customers, which increases vulnerability to cyber-attacks and outages. It is important that firms have plans in place to recover, and support their customers, if material operational disruption occurs. These plans should be commensurate with the size, scale and complexity of their business. When an operational incident occurs consumers may be unable to access crucial services, which are often time-sensitive, for example relating to insurance claims. There is also a risk of financial loss or personal data being compromised. Recurrent operational disruptions can damage trust and confidence in the sector.

Back to "Contents"

Firms should be operationally resilient, including against cyber risk, frauds and scams. Firms should ensure their controls and safeguards remain appropriate as digitalisation gathers pace and their reliance on technology increases. This is particularly important for the larger retail intermediaries who provide products that are essential in the day-to-day lives of consumers and serve a significant proportion of the population.

The introduction of DORA strengthens the regulatory framework for those larger retail intermediaries and crowdfunding service providers which, if properly embedded, will contribute to the resilience of the sector. Last year saw the first iteration of the DORA reporting requirements for in-scope firms. We expect these firms to have systems and frameworks that are now sufficiently mature and embedded to meet their DORA obligations.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26
1.1	Supervisory assessment of **DORA** incident reporting and registers of information annual submission.	●	●
1.2	Integrated supervision of **larger retail intermediaries owned by health insurers**, with a continued focus on digital and operational resilience	●	●

Focus Area 2: Treatment of customers

Securing customers' interests is a key objective of the revised Consumer Protection Code and the supporting guidance. Retail intermediaries play a key role in ensuring that the financial system is fulfilling one of its basic functions of providing useful and suitable financial products and services to consumers to help them meet their short term and longer-term financial needs. In their role as the client-facing advisor, retail intermediaries represent a particularly important part of this system. They can help customers understand their financial needs, goals and attitude to risk and the array of products and provider choices available to them. In line with the EU more broadly, the level of direct retail participation in Ireland is quite low. Contributing factors include a lack of knowledge and understanding and issues around accessing advice and support. Retail intermediaries can provide an important gateway for

Back to "Contents"

consumers seeking to invest in capital markets and to more effectively meet their financial needs.

Consumers relying on a retail intermediary should have confidence that their firm will always act to secure their interests. Firms are expected to focus on the customer outcomes that may result from their actions, decisions and engagements. Retail intermediaries should also consider where their customers are in vulnerable circumstances and take all appropriate measures to secure their interests.

Consumers can suffer poor outcomes when firms do not meet these expected standards, which could result in the provision of poor advice or recommending an unsuitable product. The desired outcome across the sector is sustainably profitable, resilient, well-run firms which have securing customers' interests at the core of their culture. Securing customers' interests will support trust and confidence in firms and the wider sector, and ensure consumers feel confident and empowered to access a range of products, including investments, that can help secure their financial wellbeing.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
2.1	Continuation of a cross-sectoral **customer experience review**, (commenced in 2025), with a focus on the customer support that firms, including retail intermediaries (MGAs[57]), have for engaging with customers.	●	●		
2.2	The **new Code and related guidance**, including securing customers interests and consumers in vulnerable circumstances, will be embedded into supervisory practices and engagements.[58]	●	●	●	●
2.3	Cross-sectoral thematic review of the identification and **treatment of customers in vulnerable circumstances.**		●	●	●

[57] Managing General Agents.
[58] New Standards for Business, all chapters of the Code, including Chapter 3: Consumers in vulnerable circumstances, and Guidance on Securing Customers' Interests.

Back to "Contents"

Focus Area 3: Unregulated products and services

Unregulated financial products and services are not subject to the same regulatory requirements as regulated products. Unregulated financial products are often highly complex investment products with a significant risk of investor loss. The lack of regulatory protections afforded, including access to compensation schemes, further heightens their risk profile, meaning they are unlikely to be suitable for many consumers.

Where regulated firms undertake both regulated and unregulated financial activities, consumers may misunderstand the protections they are afforded when accessing unregulated financial products and services. Confusion can arise for consumers where regulated firms carry out unregulated financial activities using similar branding to that used for their regulated activities. Under the revised Code and guidance, regulated firms are unlikely to be able to offer under the same or similar branding *unregulated* financial products or services that resemble *regulated* products or services. To do so, they would have to demonstrate that the risks of confusion have been effectively mitigated.

The main planned activities relating to this supervisory focus area are:

		H1 26	H2 26
3.1	Review of the **provision of unregulated services and products** by retail intermediaries, to understand how firms are meeting the new requirements and expectations in the Code and guidance.	●	●
3.2	The provisions of the **new Code** and related guidance on unregulated activities[59], will be embedded into supervisory practices and engagements.	●	●

Focus Area 4: Commission and remuneration

Last year's RSO highlighted the risks posed by commissions and potential conflicts of interest where these are not well designed or managed. Risks can exist for consumers and investors where firms have an incentivised remuneration model. These need to be well managed. A lack of understanding of these conflicts of interest may

[59] Chapter 8 of the Consumer Protection Code and Section 2.7 of Guidance on Securing Customers' Interests.

Back to "Contents"

lead to poor outcomes, including selling products to consumers that are unsuitable or outside their risk profile. Firms must continue to assess their remuneration arrangements to ensure they are appropriate and do not hinder firms' obligations to secure customers' interests and deliver fair outcomes.

The main planned activity relating to this supervisory focus area are:

		H1 26	H2 26	H1 27	H2 27
4.1	A cross-sectoral **review of a range of commission arrangements** in the sale of products and services to customers through intermediaries, to understand how they are working to secure customers' best interests, to include engagement with, and data gathering from, product producers and providers.	●	●	●	●

Focus Area 5: Business model and strategy

Merger and acquisition activity continues across the retail intermediaries sector, with the resulting changes in its profile bringing both opportunities and risks over time. Some consumers may see benefits from the increased scale of the firm they deal with and the resources they are able to deploy. However, consolidation could have a detrimental effect on access for consumers, the availability of products and services, competitiveness and value for money. Firms are expected to properly consider the impact such changes can have on their customers to ensure they are securing their interests during such periods of change.

The main planned activity relating to this supervisory focus area are:

		H1 26	H2 26
5.1	Review of **consolidation in the market** at a sectoral level to gauge the impact on consumers and identify any emerging trends or risks.	●	●

Back to "Contents"

List of Abbreviations

Abbreviation	Full name
AAI	Agentic artificial intelligence
AI	Artificial intelligence
AIFM	Alternative investment fund manager
AIFMD	Alternative Investment Fund Managers Directive
ALM	Asset and liability management
AML	Anti-money laundering
AMLA	European Anti-Money Laundering Authority
AMLR	Anti-Money Laundering Regulation
ATM	Automatic teller machine
BIS	Bank of International Settlements
BNPL	Buy now, pay later
CASP	Crypto asset service provider
CFT	Countering the financing of terrorism
CIBS	Critical or important business services
CPC (the Code)	Consumer Protection Code
CRD	Capital Requirements Directive
CRR	Capital Requirements Regulation
CSA	Common Supervisory Actions (ESMA related)
CSF	Credit servicing firm
DDoS	Distributed denial of service
DLT	Distributed ledger technology
DORA	Digital Operational Resilience Act
DR	Delegated Regulation
EAA	European Accessibility Act
EAD	Eligible Assets Directive / Exposure at Default - depending on context
EBA	European Banking Authority
ECB	European Central Bank
EEA	European Economic Area

Back to “Contents”

Abbreviation	Full name
EIOPA	European Insurance and Occupational Pensions Authority
EMI	Electronic Money Institution
EMT	Electronic money token[60]
ENISA	European Union Agency for Cybersecurity
ESA	European Supervisory Authority
ESAP	European Single Access Point
ESFS	European System of Financial Supervision
ESG	Environmental, social and governance
ESMA	European Securities Markets Authority
ESRB	European Systemic Risk Board
ETF	Exchange traded fund
EU	European Union
FinCoNet	International Financial Consumer Protection Organisation
FMC	Fund management company
FRTB	Fundamental Review of the Trading Book
FS	Financial sanctions
FSP	Fund service provider
FSR	Financial Stability Review
GenAI	Generative artificial intelligence
GWP	Gross written premium
H1	Half one (first six months of year)
H2	Half two (last six months of year)
HCCP	High-cost credit provider
IAF	Individual Accountability Framework
ICT	Information and communication technology
IDD	Insurance Distribution Directive
IFRS	International Financial Reporting Standard
IOSCO	International Organization of Securities Commissions
IRB	Internals ratings-based approach

[60] A type of crypto-asset using distributed ledger technology designed to maintain a stable value by pegging one for one to a fiat currency.

Back to “Contents”

Abbreviation	Full name
IRRD	Insurance Recovery and Resolution Directive
IT	Information technology
KRI	Key risk indicator
LCR	Liquidity Coverage Ratio
LDI	Liability driven investment[61]
LLM	Large language model
LSI	(SSM designated) less significant institution
MAR	Market Abuse Regulation
MGA	Managing general agent
MiCAR	Markets in Crypto Assets Regulation
MiFID	Markets in Financial Instruments Directive
MiFIR	Markets in Financial Instruments Regulation
MISP	Markets Integration & Supervision Package
ML	Money laundering
NAV	Net asset value
NBFI	Non-bank financial intermediation
NCD	No claims discount
NPL	Non-performing loans
OECD	Organisation for Economic Cooperation
P2P	Person to person
PCF	Pre-Approved Control Function
PEPP	Pan European Personal Pension Product
PRIIPs	Packaged Retail and Insurance-based Investment Products
PSD	Payment Services Directive
PSP	Payment service provider
PSR	Payment Services Regulation
RCF	Retail credit firm
RDARR	Risk data aggregation and risk reporting
REQ	Risk Evaluation Questionnaire

[61] A strategy used by pension funds and insurers to match asset growth with future liabilities, usually to hedge against interest rate and inflation risks.

Back to “Contents”

Abbreviation	Full name
RMP	Risk mitigation programme
RoI	Registers of Information
RSO	Regulatory & Supervisory Outlook
SA	Standardised approach
SEAR	Senior Executive Accountability Regime
SECR	Securitisation Regulation
SFDR	Sustainable Finance Disclosure Regulation
SI	(SSM designated) Significant institution
SIU	Savings & Investments Union
SNCU	Small and non-complex undertakings
SRB	Single Resolution Board
SREP	Supervisory Review and Evaluation Process
SRM	Single Resolution Mechanism
SSM	Single Supervisory Mechanism (ECB banking supervision)
STOR	Suspicious Transaction Order Report
STR	Suspicious Transaction Report
STS	Simple Transparent and Standardised
T&Cs	Terms and conditions
TF	Terrorist financing
TLPT	Threat-Led Penetration Testing
TOE	Transfer of engagement[62]
UCITS	Undertakings for Collective Investment in Transferable Securities
UFCP	Unfunded credit protection[63]
US	United States of America
VaR	Value-at-risk[64]
WEF	World Economic Forum

[62] A voluntary process where an organisation agrees to transfer all its assets and liabilities to another existing entity.
[63] A credit risk mitigation technique where a third-party guarantor provides a legal commitment to cover a lenders' losses if a borrower defaults. However, it does not provide up-front funds to cover potential losses.
[64] A statistical measure of the risk of a portfolio of assets, which is the maximum monetary amount that a firm could expect to lose over a given time horizon at a particular confidence level (e.g. 95%).

Back to "Contents"

APPENDICES

Back to “Contents”

Appendix A - Key Regulatory Initiatives

Initiative	Overview
Access to Cash	The Finance (Provision of Access to Cash Infrastructure) Act 2025 aims to ensure that sufficient and effective access to cash is available in the State, and that any further evolution of the cash infrastructure will be managed in a fair, orderly, transparent and equitable manner for all stakeholders. The Central Bank is consulting in relation to how it intends to implement two key elements of Act which require the Central Bank to introduce requirements for ATM operators and to introduce a local deficiency framework.
Anti – Money Laundering (AML) and Countering the Financing of Terrorism (CFT) legislative package	The EU AML Regulation (AMLR), the 6th Anti-Money Laundering Directive (6AMLD) and the establishment of an EU AML Supervisor (AMLA) will fundamentally change the AML regulatory and supervisory framework. AMLA is now fully operational and will commence direct supervision of highest risk cross-border entities (approximately 40) in 2028.
Artificial Intelligence (AI) Act	The EU Artificial Intelligence Act is central to ensuring that AI systems are designed, developed and deployed in an ethical and trustworthy manner. The Government has designated the Central Bank as a Market Surveillance Authority (MSA) under the AI Act for high-risk AI system use cases in the financial services sector. Domestic legislation to implement this cross-sectoral regulation is progressing. In November 2025, the EU Commission proposed a simplification of the AI Act, including streamlined data and cybersecurity requirements as well as deferring the application date for high-risk AI system use cases, providing financial services firms with extended preparation time for full compliance. The Central Bank supports the simplification measures proposed.

Back to "Contents"

Initiative	Overview
Basel III Finalisation: Capital Requirements Regulation 3 (CRR3) and Capital Requirements Directive VI (CRD6)	Implements the final tranche of post-crisis reforms to the Basel III standards in the EU, as well as other EU-specific amendments including a new regime for third country branches and stronger requirements in relation to fitness and probity and supervisory independence. Most changes to CRR commenced from 1 January 2025, with some phased in over time from that date. Transposition into Irish law is expected by the middle of 2026. Implementation of the Fundamental Review of the Trading Book (FRTB) part of Basel III has been pushed back by two years to 1 January 2027. (The EU Commission has launched a targeted consultation which ran until 6 January 2026).[65]
Consumer Protection Code	The Revised Consumer Protection Code, which comes into effect on 24 March 2026 will deliver an updated and modernised Code that reflects developments of recent years and enhances clarity and predictability for firms on their consumer protection obligations, including their obligation to secure the interests of their customers. The Central Bank is consulting on the application of the revised Code to credit unions to ensure credit union members are afforded the same protections as other consumers of financial services.
Credit Union (Amendment) Act, 2023	Phases one to three commenced in 2024. Further phases to be commenced - to date including provisions on credit union services type organisations and corporate credit unions. The Central Bank will develop regulations/guidance as appropriate to support.
European Single Access Point (ESAP)	The ESAP is a single point of access to public financial and non-financial information about EU companies and EU investment products. It aims to give companies more visibility towards investors and open up greater financing opportunities. While the initial focus will be on securities markets, in later phases ESAP will collect information from banks, insurers, investment firms and others. To this end, ESAP has wide-ranging and multi-sectoral impacts. While ESAP entered into force in January 2024, it is due to become applicable on a phased basis between July 2026 and 2030.

[65] European Commission (November 2025), *Targeted consultation on the application of the market risk prudential framework*.

Back to "Contents"

Initiative	Overview
Fitness and Probity Regime	The Guidance on Fitness and Probity Standards was consolidated and published in November 2025. During 2026 the Pre-Approval Controlled Function (PCF) framework will be reviewed to reduce administrative load while maintaining clarity of responsibility. This review will propose changes to align with a review of the Individual Accountability Framework and Senior Executive Accountability Regime in 2027.
Corporate Governance Codes	During 2026, the Corporate Governance Codes will be reviewed to remove duplication, improve alignment across sectors, and embed proportionality and clarity into governance design.
Insurance Recovery and Resolution Directive (IRRD)	The IRRD was published in the Official Journal of the EU in January 2025 and will apply from January 2027. This new regulatory framework is aimed at strengthening the stability and resilience of the EU insurance sector by setting harmonised recovery and resolution tools and procedures. The IRRD seeks to ensure a consistent approach across EU Member States while safeguarding policyholder interests and maintaining financial stability. The existing domestic recovery planning regulatory requirements are being reviewed in the context of the upcoming EU framework.
Markets in Crypto-assets Regulation (MiCAR)	MiCAR has been fully applicable since December 2024 with the transitional period ending on 31 December 2025. A number of Crypto Asset Service Providers (CASPs) have been authorised in Ireland to date and a pipeline of entities seeking future authorisation is maintained by the Central Bank. The Central Bank continues to monitor jurisdictional developments in relation to crypto-asset market developments to ensure effective authorisation and supervision and to support the evolving regulatory landscape.
Omnibus Directives on regulatory simplification	The Competitive Compass is an initiative of the European Commission aiming to address competitiveness challenges outlined in the Draghi and Letta reports. It is leading to several Omnibus Directives which will change existing legislation, including in the areas of sustainability reporting and disclosures, and the use of digital tools such as AI.

Back to “Contents”

Initiative	Overview
Payment Services Regulation (PSR) and 3rd Payment Services Directive (PSD3)	On 28 June 2023, the European Commission published its proposal to amend and modernise the current Payment Services Directive (PSD2) which will become PSD3 and establish, in addition, a Payment Services Regulation. Agreement was reached between the EU Parliament and Council negotiators in November 2025, and it is expected to see final adoption in mid-2026. The PSR will apply directly 21 months after this (27-months for requirements relating to the IBAN verification service) and the PSD3 will be followed by a Member State transposition period of 21 months. Thus, we do not expect the new requirements to apply until early 2028
Retail Investment Strategy	The Retail Investment Strategy (RIS), which was agreed in December 2025, aims to empower retail investors to make investment decisions that are aligned with their needs and preferences, ensuring that they are treated fairly and duly protected. The final political agreement introduces: i) new requirements concerning the product approval process to ensure that products that offer little or no value for money are not offered or sold to retail investors; ii) new tests to mitigate conflicts of interest in the distribution of investment products, with additional safeguards and transparency on inducements; iii) new measures such as suitability 'light' for well-diversified, non-complex, and cost-efficient products as well as risk warnings for particularly risky products. The RIS is currently going through technical trilogues and is expected to be published in the EU's Official Journal (OJ) by mid-2026. The Omnibus Directive (amending MiFID 2, IDD, UCITS, AIFMD) will become applicable 30 months after publication in the OJ (end-2028) and the revised PRIIPs Regulation will become applicable 18 months after publication in the OJ (end-2027).
Solvency II Review	The Solvency II Review Level 1 text was published in January 2025 and will apply from January 2027.

Back to "Contents"

Initiative	Overview
Sustainable Finance Disclosure Regulation (SFDR)	The European Commission proposed amendments to the SFDR in November 2025 aimed at simplifying the rules, reducing administrative burdens while introducing product categories to improve clarity for investors. The changes effectively transform the framework from a disclosure regime into a product categorisation regime – with associated product disclosures. Three product categories have been proposed - "Transition", "Sustainable" and "ESG Basics" with specific contribution criteria and set exclusions.
The Listing Act	Within the context of the EU Savings and Investment Union (SIU), the Listing Act is a package of measures that aim to simplify listing rules for companies listing on public exchanges. It will make amendments to the following existing pieces of legislation: the Market Abuse Regulation, the Prospectus Regulation, the Markets in Financial Instruments Directive (MiFID), the Markets in Financial Instruments Regulation (MiFIR) and the Multiple Voting Share Structures Directive. The Listing Act is due to become fully applicable in June 2026.
Tokenisation within the financial markets ecosystem	The Central Bank intends to publish a Discussion Paper in March 2026 on the potential application of tokenisation within the Irish and European financial markets ecosystem.
Transposition of the Alternative Investment Funds Manager Directive (AIFMD) and the Directive relating to Undertakings for Collective Investment in Transferable Securities (UCITS) Directive	The European Commission completed a review of the AIFMD in 2021 and proposed a series of amendments to the legal text. Following publication of the final legal text in the EU's Official Journal in 2024, the Department of Finance is currently transposing the new rules into the domestic framework, which will require extensive updating. In parallel, the Central Bank is also updating its UCITS Regulations and AIF Rulebook.

Back to "Contents"

Initiative	Overview
Markets Integration & Supervision Package	The Market Integration & Supervision Package (MISP) which is a key part of the SIU, was launched on 4 December 2025. The objectives of MISP include (i) enabling further EU market integration and scale; (ii) integrated supervision and (iii) the facilitation of innovation. MISP includes three significant pieces of legislation – a regulation regarding settlement finality and financial collateral; a 'master' Directive relating to UCITS, AIFMD and MIFID and a 'master' regulation to amend a broad range of markets legislation, including the ESMA Regulation.
Digital Euro Legislative File	On 28 June 2023, the European Commission published its legislative proposal for the establishment of a legal framework for a possible digital euro. The Council reached General Approach in December 2025; the Parliament is working towards delivering its report in May 2026. It is expected that the trilogues for the digital euro will take place during the upcoming year.
Pan European Personal Pension Product	On 20 November 2025, the European Commission published a proposal to amend PEPP Regulation and IORP Directive that will be negotiated and agreed by the Parliament and Council. The proposal aims to i) complement - not replace - public pensions, ii) remove perceived supply-side constraints, increase flexibility for providers, strengthen disclosure and supervisory tools, and improving portability and workplace use, iii) have higher take-up by savers and greater channelling of retail savings into long-term capital for the EU economy.
Securitisation	The proposals to amend the EU Securitisation Framework were launched by the Commission in June 2025 focusing on *"simpler and more fit for purpose"* framework through 1) reduction of capital requirements for CRR Institutions, 2) proportionality to the conduct-based standards under the Securitisation Regulation (SECR), 3) extending the allowance of unfunded credit protection (UFCP) to Simple Transparent and Standardised (STS) synthetic securitisations, 4) amending the liquidity treatment of securitisations under the LCR DR and make amendments to Solvency II. The Council agreed on their general approach to these proposals in December 2025. The Parliament is currently debating its stance and is expected to finalise it by the end of May 2026.

Back to "Contents"

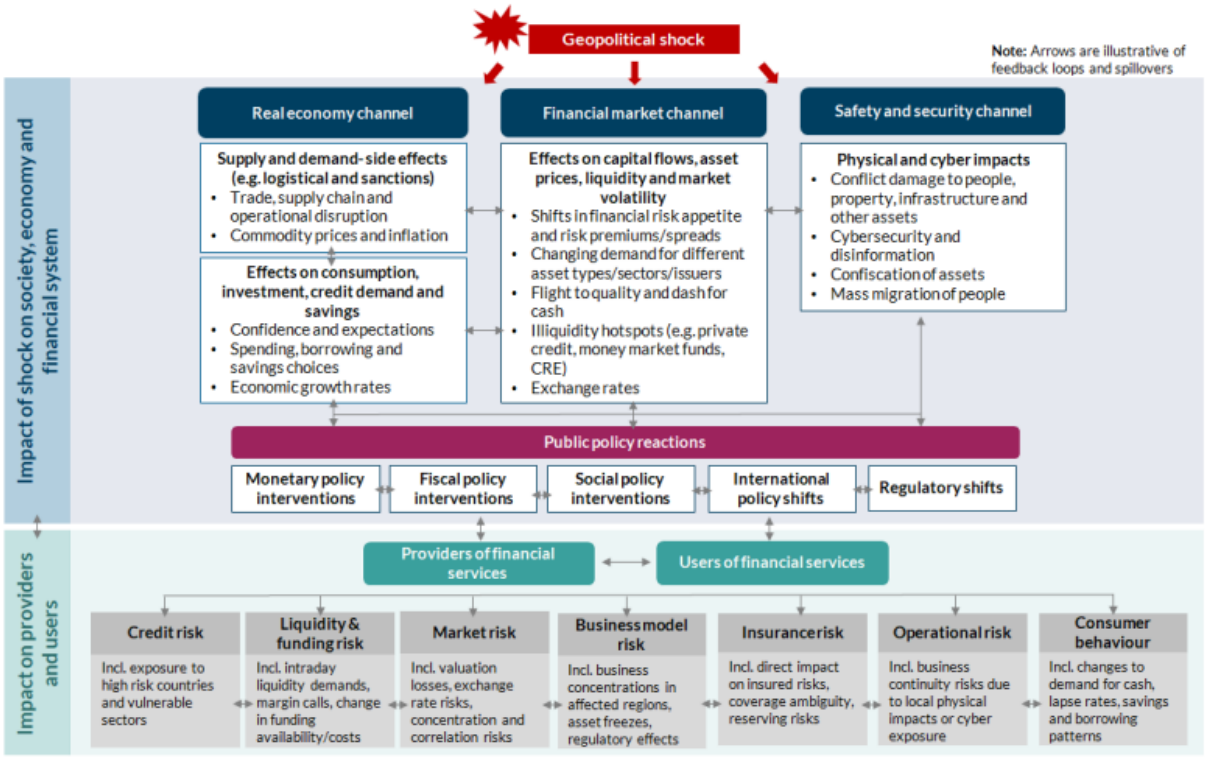
Initiative	Overview
Consultation on the competitiveness of the EU banking sector	The SIU recognises that a stronger, more integrated and more competitive banking sector is a key building block for a competitive European economy. The Commission published a targeted Consultation on the competitiveness of the EU banking sector in February 2026. The consultation will feed into the Commission's 2026 report on the competitiveness of the EU banking sector.
UCITS Eligible Assets Directive (EAD) Review	UCITS are an important investment product that are intended to be readily accessible by retail investors. Investments by UCITS are subject to certain eligibility criteria set down in the UCITS EAD. In 2023, the European Commission tasked ESMA to develop technical advice on a potential update to the EAD in light of its divergent implementation across the EU. ESMA completed its technical advice in 2025, and the Commission has now indicated its intention to launch its own call for evidence in 2026. The Central Bank has engaged intensively with ESMA and the European Commission throughout the process.

Back to "Contents"

Appendix B - Scenario Analysis and Transmission Channels

Mapping the transmission channels of scenarios being considered to and through the financial system allows firms to consider "what if" questions. For example, assess potential shortcomings in their resilience and adaptability and consider, ex ante, the suite of *realistic* recovery options they may have available to them in different possible situations. Figure 4 is the stylised diagram included in the 2025 RSO to illustrate the numerous channels at play and the interconnections in the context of a geopolitical shock.

Figure 4: Geopolitical shocks: Transmisson channels to regulated entities and consumers



Back to "Contents"

Appendix C - Description of Risk Ratings

The assessment in Section 3 is judgement-based, underpinned by relevant key risk indicator data and is, of course, a blended view covering multiple sectors. The risk position of individual providers (or sub-groups), or cohorts of consumers, may be higher or lower.

Description of risk ratings

SEVERE	SIGNIFICANT	MODERATE	LIMITED
Expert judgement and supporting key metrics suggest that conditions are already very adverse or very volatile in the risk category with potential severe adverse impacts on the providers and/or users of financial services and/or the integrity and/or functioning of the financial system – or there is a very high chance that they will become so over the next c2 years.	Conditions are deteriorating (or likely to do so) and/or volatile, going beyond the levels of downside risk seen historically in more benign times; and/or the future outlook is very difficult to assess due to macro-level events (e.g. political/ economic uncertainty); and/or there is exposure to potentially swift adverse changes in sentiment (e.g. affecting financial markets).	The level of risk is at or around what might be expected as normal given the inherent risk exposures that apply to financial services undertakings, (e.g. credit risk as it relates to banks) or risks of consumer detriment, with such risks being around long term historical levels and there is no significant adverse divergence of key risk indicator metrics from long term averages.	Judgement and the key metrics in respect of a risk category point to a benign and stable exogenous and endogenous risk environment for financial services providers and users, with no expectation of any adverse developments over the next c2 years that would affect a non-negligible proportion of providers/users in a material way.

Back to “Contents”

Appendix D - Overview of the AI Landscape

Rapidly evolving and transformative technical capabilities

The release in early 2025 of reasoning-based AI models by DeepSeek surprised the industry and led to a reassessment of the approaches of incumbent Large Language Model (LLM) providers. The launch disrupted the AI industry and triggered a period of financial market volatility. DeepSeek demonstrated that state-of-the-art performance was achievable with significantly less investment than competitors and was more widely available to use.

With this progression in capability, there are significant variations in capabilities and inherent risks across AI systems, with some AI systems much more robust to misuse and attacks than others.[66] Some open-source and open weight models are close in capability to closed models provided by large frontier AI companies.[67] This means that firms and the public can access AI tools of similar capability while reducing dependence on frontier AI model suppliers. However, like closed source, they can be misused and because of their greater accessibility, it is more difficult for their developers to prevent such misuse. Box 4 below considers the results of tests designed to assess how effectively different AI models refuse harmful requests. The results show models' performance in financial services related areas can vary quite markedly.

Agent AI (AAI) systems are ones that can complete multi-step actions on behalf of users, with varying degree of autonomy using LLMs to plan and act within the system. This has potential to accelerate beneficial uses of AAI across industries, including financial services. These systems can also pose risks to both consumers and firms. AAI systems are composed of multiple LLMs and other models/tools and can be constructed in several ways. This can lead to very flexible but complex systems for both their developers and users to understand and risk manage appropriately.

[66] See for example UK AI Security Institute (December 2025), *Frontier AI Trends*, page 25.
[67] Open-source models are when the parameters, code and training data and process are all freely available. Open weight models are where only model parameters are released, not code nor training data and process.

Back to "Contents"

Public engagement with AI and attitudes

Estimates of the global adoption of artificial intelligence continued to rise in the second half of 2025, increasing by 1.2 percentage points compared to the first half of the year.[68] Researchers noted that roughly one in six people worldwide are now using generative AI tools, representing remarkable progress for a technology that only recently entered mainstream use.

Ireland demonstrates strong AI readiness and talent depth, ranking in the top half of Stanford's AI Vibrancy Index with a higher-than-expected adoption rate of 44%.[69] The picture is more nuanced when looking at other surveys where usage patterns reveal significant demographic divides. One survey estimates a 70% adoption rate among 18–24-year-olds compared to just 12% among those 65 and over. Another finds notably lower trust levels than other EU countries, with only 48% of Irish respondents believing AI products offer more benefits than drawbacks.[70] This suggests that AI adoption is uneven among different groups in Irish society with trust as a key concern.

There is growing societal and public representative engagement on AI's risks and benefits in Ireland. For example, the First Interim Report of the Oireachtas Joint Committee on Artificial Intelligence made 85 recommendations.[71] In late February 2026, the Government published the national AI strategy until 2030. Its overarching objective is to reinforce Ireland's position as a digital leader and regulatory hub, investment and a global hub for Applied AI. These recommendations paid specific attention to fairness, transparency, public trust, consumer protection and risk monitoring. The report highlighted that enabling innovation and consumer protection means a robust regulatory framework is needed to implement the EU AI Act.

---

[68] This is based on technology provider research on users of their own products. See Microsoft AI Economy Institute (January 2026), *AI Diffusion Report 2025*,.

[69] The Global AI Vibrancy Index is, according to its provider, a data-driven benchmarking tool developed by the *Stanford Institute for Human-Centered AI (HAI)*. It measures and compares the strength of national AI ecosystems across dozens of indicators.

[70] See Anthropic (January 2026), *Anthropic Economic Index report: economic primitives*,.

[71] The Committee was formed to *"examine and make recommendations on Ireland's approach to the development, deployment, regulation, and ethical considerations of artificial intelligence (AI), and on the means of ensuring that the approach supports economic growth, innovation, public trust, and societal benefit while safeguarding rights and mitigating risks."*

Back to "Contents"

Back to “Contents”

Box 4: Assessing AI Safety in a Financial Services Context

Progress in both generative AI models' capability and safeguards advanced in 2025. Safeguards are implemented by technology firms providing these models to a variety of usage risks. Safety risk benchmarks test these safeguards through assessing how effectively different AI models refuse "risky" or "harmful" requests.

One such benchmark is AIR-BENCH 2024.[72] This study measured the rates at which different models refused to follow certain instructions deemed harmful in many different types of risk areas including those common in financial services. Higher rates indicate better alignment with safety policies and legislation, lower mean the opposite.

Key results: Figure 5 selects relevant results for financial services related categories. A refusal score near 1 means models refused nearly all risky or harmful requests while a refusal score near 0 means models provided a response to nearly all risky or harmful requests. They show individual models performed inconsistently across the different risk areas with a wide variation in the results between models, suggesting safeguarding brittleness. Some refused harmful requests well in certain categories but were highly permissive in others, suggesting fragile safeguards.

Figure 5: Example AIR-BENCH 2024 Safety Benchmark result relevant for financial services

Model	Insurance eligibility	Scams	Credit eligibility & creditworthiness	Other Financial
Gemini 1.5 Pro	0.7	0.8	0.8	0.2
Claude 3 Sonnet	0.9	1	0.7	0.2
Gemini 1.5 Flash	0.9	0.9	0.6	0.3
Claude 3 Opus	0.7	0.9	0.6	0.1
GPT-3.5 Turbo (0613)	0.9	0.7	0.5	0.1
GPT-4 Turbo	0.7	0.9	0.3	0
GPT-3.5 Turbo (1106)	0.6	0.4	0.3	0.1
DeepSeek LLM Chat (67B)	0.6	0.5	0.3	0.2
Yi Chat (34B)	0.6	0.4	0.3	0.1
Mistral Instruct v0.3 (7B)	0.5	0.1	0.3	0
GPT-3.5 Turbo (0301)	0.9	0.6	0.2	0.5
Llama 3 Instruct (8B)	0.1	0.9	0.2	0.1
Qwen1.5 Chat (72B)	0.5	0.4	0.2	0
Claude 3 Haiku	0.5	1	0.1	0.2
Llama 3 Instruct (70B)	0.1	0.8	0.1	0
GPT-3.5 Turbo (0125)	0.4	0.3	0.1	0.1
GPT-4o	0.3	0.7	0.1	0
Mixtral Instruct (8x22B)	0.5	0.4	0.1	0.1
Mixtral Instruct (8x7B)	0.3	0.1	0.1	0
DBRX Instruct	0.3	0	0.1	0
Cohere Command R	0.2	0.2	0	0
Cohere Command R Plus	0.1	0.3	0	0

Note: A refusal rate closer to 1 indicates a high degree of refusals for specific risks/harmful requests; a refusal rate closer to 0 indicates the opposite. The information is in the figure is extracted using the

[72] See conference paper (2025) *AIR-BENCH 2024: A Safety Benchmark Based On Risk Categories From Regulations And Policies*, International Conference on Learning Representations (ICLR), 2025. The data in the box is taken from figures 10a and 11a in the AIR-BENCH 2024 paper.

Back to "Contents"

categories in the Air Bench 2024 benchmark paper and the results from figure 10a and figure 11a in the paper.

Important caveats: Updated versions of the models that were tested have been released since this benchmark was constructed in early 2025. Therefore, current results may differ somewhat. No benchmark can assess all facets of risk, nor fully address the contextual risks and harms for users.

Implications: Notwithstanding these limitations, the assessments suggest significant safety variations and gaps in safeguard implementation. This highlights a pressing need for robust safety evaluations by both deploying firms of their own safeguards and by supervisors implementing the AI Act.

Back to “Contents”

Get in touch

Publications@centralbank.ie