RSM

CBI Supervisory Outlook 2026

Banking sector

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

Banking sector

Regulatory & Supervision Outlook (key areas of focus by the CBI for 2026):

1

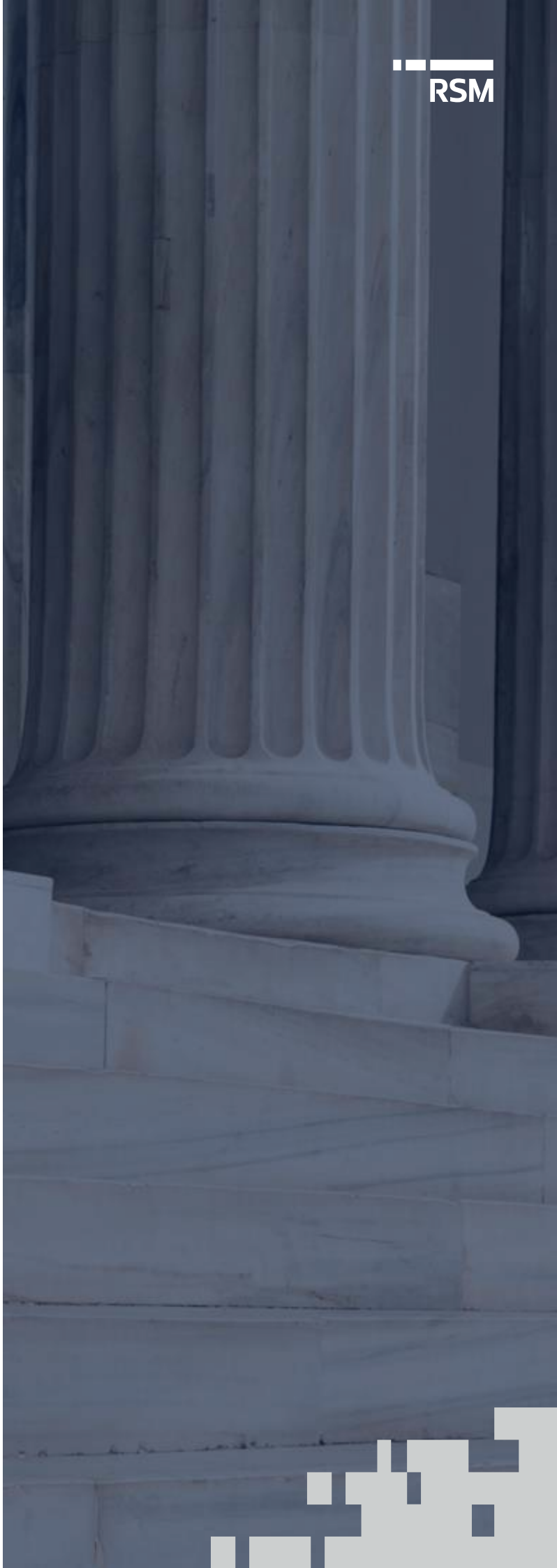
The Central Bank of Ireland's 2026 Regulatory & Supervisory Outlook is published against a backdrop of accelerating structural change, geopolitical fragmentation, rapid technological innovation, and evolving consumer expectations.

These forces are reshaping the risk environment across the entire financial system, and the CBI has made clear that firms must demonstrate resilience, strong governance, and the ability to operate in a rapidly shifting environment.

2

Operational and cyber risks remain the most elevated cross sector threats, fuelled by rising digitalisation, complex outsourcing chains and geopolitical instability.

Alongside this, consumer protection, financial crime, climate risk, and the responsible adoption of AI are central pillars of the supervisory agenda for 2026.



Introduction

What follows are the banking specific considerations for 2026:

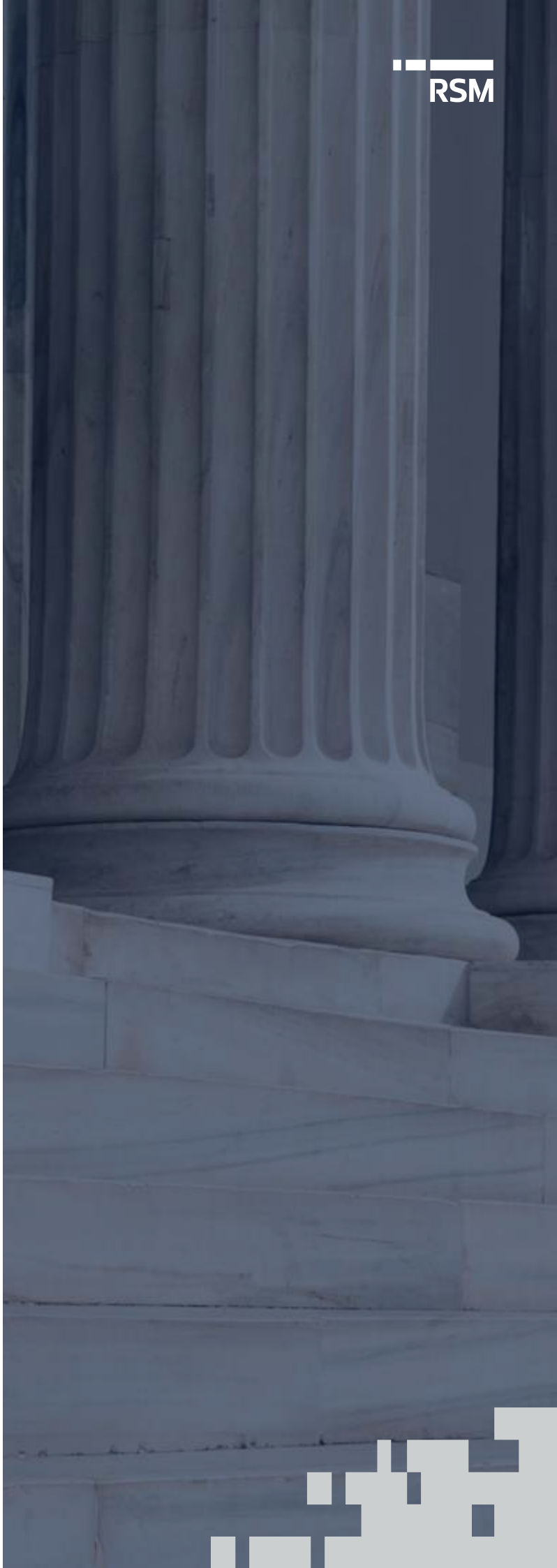
- The Irish banking sector enters 2026 in a position of broad financial resilience, supported by strong capital positions, improved profitability and strengthened balance sheets. Yet this resilience is being tested by a rapidly evolving external environment. Banks face growing competition from digital-only firms, fintech innovators and non-bank financial institutions, all of which are reshaping customer expectations and intensifying pressures on legacy business models. Additionally, impending regulatory changes—such as CRD6 requirements for third country institutions—are expected to prompt structural adjustments within parts of the sector. These dynamics heighten the need for strategic clarity, robust governance, and board oversight.

- The supervisory agenda for 2026 places significant emphasis on **operational and cyber resilience**, which the CBI identifies as a critical vulnerability given the sector's heavy reliance on cloud technologies, key third-party service providers, and large-scale digital transformation programmes. Banks are expected to demonstrate full and effective implementation of DORA, strengthen ICT governance, and address shortcomings uncovered by prior cyber and outsourcing inspections.

- At the same time, **consumer protection concerns remain persistent**, particularly as more customer journeys shift to digital channels. The revised Consumer Protection Code, effective March 2026, will be a focal point for supervisory testing across areas such as complaints handling, sales through banking apps, treatment of vulnerable consumers, and accuracy of disclosures.

- The CBI also highlights the need for banks to sustain prudent **financial resilience**, including ongoing monitoring of credit risks (especially in mortgages and short-term lending), asset valuations, climate related exposures, and data quality issues that impede reliable risk reporting.

- Finally, **financial crime and market integrity** risks are rising, driven by increasingly sophisticated fraud typologies and cross sector AML concerns. The CBI will intensify AML inspections, enhance sectoral data collection, and scrutinise wholesale market conduct and surveillance frameworks. Together, these priorities underscore a supervisory environment that demands banks be resilient, transparent, technologically capable, and customer centric.



Key 2026 supervision themes

Consumer protection and risk - The CBI continues to see harm arising from poor customer treatment, weak governance, errors, and ineffective communication, particularly as banks move to digital-only channels. The revised Consumer Protection Code (effective March 2026) will be enforced through thematic reviews focusing on complaints handling, treatment of vulnerable customers, sales via banking apps, current account servicing, and BNPL and mortgage suitability..

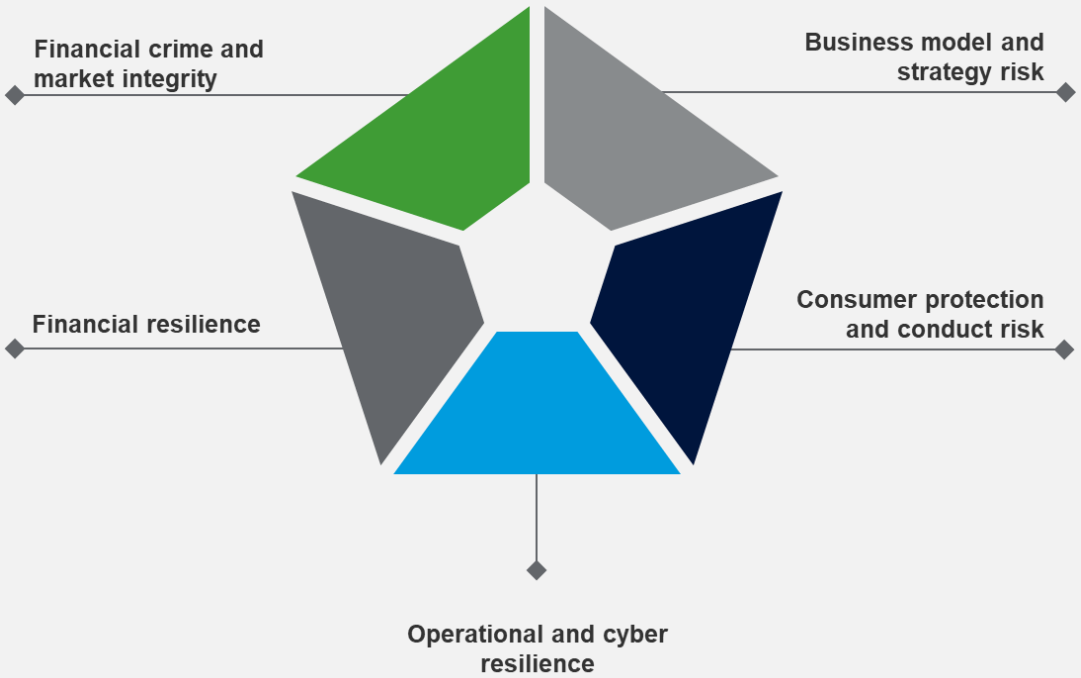
Operation AI and cyber resilience- A key risk for 2026, reflecting geopolitical volatility and heavy reliance on third-party ICT and cloud services. The CBI will conduct cyber security inspections, threat-led penetration testing, ICT outsourcing and cloud dependency reviews, DORA implementation testing, and outage management monitoring.

Financial resilience - Supervisory focus will include SREP assessments (including climate and nature risks), capital and liquidity adequacy analysis, credit risk, loan origination and mortgage lending stress, RDARR (data quality) remediation, and AI model governance in credit and trading.

Financial crime and market integrity - Banks face inherently high exposure to AML/CFT inspections. The CBI will require enhanced REQ data collection, sector-wide fraud reviews, and market abuse surveillance, particularly for wholesale banks.

Business model and strategy risk - Banks face intense competition from fintech firms, non-banks, and new digital entrants. The CBI will examine strategic changes, board oversight, risk appetite alignment, and readiness for CRD6-related structural changes.

Figure 1: Key 2026 supervisory themes



Heat map of key regulatory and supervisory risks in the banking sector.

Key risk area of focus for 2026	Severity	Rational behind the 2026 key focus risk areas	Further consideration
Operational and cyber resilience	Severe	Banks increasingly rely on digital channels, cloud services, and complex third-party arrangements. The CBI highlights that geopolitical tensions and rising cyber attacks mean operational outages are more likely—and banks must remain able to deliver critical services 24/7.	The CBI notes a rise in cyber threats, outages and DDoS attacks targeting Irish banks, as well as high dependency on cloud and IT outsourcing. These factors make disruptions more likely and potentially more severe. Banks must implement DORA, improve ICT governance, and prove they can recover quickly from disruptions.
Consumer protection / conduct	High	Banks' digital transformation and reduced physical service channels increase the risk of errors, poor customer communication, and vulnerability related harm. The CBI continues to find weaknesses in how banks treat customers.	Reviews show recurring issues: poor complaints handling, unclear app-based product disclosures, weak treatment of vulnerable customers, and repeat errors driven by poor governance. The revised Consumer Protection Code will intensify scrutiny.
Financial crime / AML	High	Banking channels are prime targets for organised crime, fraudsters, and money launderers. Increased digital payments, scams and cross border flows create opportunities for exploitation.	The CBI highlights a sharp rise in scams and fraud across the financial system. AML/CFT frameworks vary between banks, and the sophistication of criminal networks is increasing. The CBI will use enhanced AML REQs and targeted inspections to address gaps.
Data and AI risk	High	Banks increasingly use advanced models and AI for credit decisions, trading, and operational processes. Weak data governance or poor oversight can lead to biased decisions, regulatory breaches, or prudential misjudgements.	The CBI observed deficiencies in data quality, model risk management, and explainability. AI adoption is accelerating faster than governance frameworks. Poor model controls can lead to customer harm and financial losses.
Credit and market risk	Moderate	While banks are currently well capitalised, the environment remains uncertain. Rising geopolitical tensions, potential asset repricing, mortgage borrower vulnerability and interest rate transitions pose risks.	The CBI warns of "stretched valuations," possible market corrections (especially AI linked stocks), and mortgage borrower stress. Climate risks also affect collateral values. But banks' stress test performance and provisioning currently mitigate severity.
Climate and environmental risk	Moderate	Climate events are increasing in frequency and severity. Banks face both physical risks (flood-damaged collateral) and transition risks (stranded assets, regulatory changes).	The CBI notes that storms and flooding are already causing significant losses in Ireland. Some banks have advanced climate risk integration, but others lag behind. The risk level rises over the long term if not addressed.

What the CBI's 2026 outlook means for the banking sector

The CBI has emphasised three overarching expectations for banks in 2026

Banks must evidence resilience-not just assert it

The CBI highlights that Ireland's financial system is now more exposed to international transmission channels, including cyber-attacks, market volatility, and operational outages driven by third party dependencies. Supervisory scrutiny will focus on the credibility of operational resilience frameworks, recovery capabilities, and the integration of climate, liquidity, and valuation risks into strategic planning.

Governance and accountability must keep pace with digital transformation

Board oversight of technology, outsourcing, cyber security, and model risk has not always matched the scale of operational change. With DORA, the revised Consumer Protection Code, CRD6 branch restructuring, and the EU AI Act all taking effect over the next 24 months, the CBI expects Boards to take explicit responsibility for technology enabled risks, ensuring that oversight frameworks, skills, and reporting are sufficiently robust.

A customer centric operating environment is now a regulatory minimum

The CBI has strengthened expectations around digital customer journeys, treatment of vulnerable customers, error management, and complaints handling—underscored by the CPC 2026 requirements. Weaknesses in disclosures, product suitability, or digital only service channels will trigger thematic reviews and potential enforcement.

In essence, 2026 marks a pivot from "establishing frameworks" to "proving capability." Banks must demonstrate that resilience, governance, and culture are embedded in day-to-day operations and evidenced through data, testing, and outcomes—not just policy statements.

Immediate actions for banks to take in 2026 (Q2–Q4 priority roadmap)

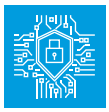
Strengthen operational and cyber resilience ahead of DORA enforcement	• Finalise and validate Critical/Important Business Services (CIBS) mappings. • Ensure incident classification, response and reporting processes align fully with DORA expectations. • Conduct scenario tests and ensure credible exit strategies for cloud and outsourced providers.
Complete CPC 2026 readiness testing	• Assess digital customer journeys for suitability, transparency, and fairness. • Review frameworks for identifying and supporting vulnerable customers. • Strengthen complaints handling and remediate root cause issues.
Prepare for CRD6 third-country branch restructuring impacts	• Identify whether Article 21c requirements affect group structures. • Develop impact assessments covering risk appetite, governance, and operational design.
Enhance financial and credit risk resilience	• Re assess mortgage book vulnerability, particularly in light of borrower affordability risks and macro uncertainty. • Validate valuation methodologies for loans, market positions, and capital buffers—especially given the CBI's concerns about "stretched valuations" and NBFI amplification risks.
Prepare AI governance for the EU AI Act	• Inventory all AI driven systems, especially high-risk creditworthiness and underwriting models. • Implement explainability, bias testing, and oversight frameworks aligned to the Act.
Strengthen AML/CFT and fraud controls in response to rising scam activity	• Prepare for enhanced AML/CFT REQs with improved data quality. • Expand fraud detection capabilities, including AI enabled anomaly detection. • Review cross border flows and sanctions screening controls.

Areas of expected supervisory intensification in 2026

The Regulatory and Supervisory outlook (RSO) and external supervisory commentary provide a strong indication of where the CBI will apply heightened pressure, focus on persistent weaknesses, and escalate interventions.

Area	Rational behind the 2026 key focus risk areas
1. Cloud dependency, ICT outsourcing and third-party risk	The CBI remains concerned about the sector's concentration on a small number of cloud and ICT providers, increasing systemic vulnerability. Banks should expect deeper inspection of exit plans, dependency mapping, sub outsourcing oversight, and testing of failover capabilities.
2. Model risk management and AI governance	Given expanding use of AI and advanced models across credit, AML, trading and customer interaction channels, the CBI will intensify reviews of: • Model validation practices • Explainability and bias controls • Reliance on group level oversight • Data quality and lineage, AI is explicitly framed as a cross-cutting risk area in the RSO and related legal commentary.
3. Treatment of vulnerable customers and digital conduct risk	With increased digital only service models, the CBI intends to address recurring issues in digital disclosures, complaints handling, and error remediation. The CPC 2026 requirements will drive thematic reviews across the sector.
4. Market valuation, liquidity, and leverage risk	The CBI Highlights elevated risk relating to asset valuations, liquidity conditions and leverage across the financial systems, driven by geopolitical uncertainty and shifting market sentiment. While balance sheets remain broadly resilient, vulnerabilities may emerge through rapid repricing of assets, increase volatility, and amplification efforts arising from interconnected exposures – particularly involving non-bank financial institutions (NBFI's) Supervisory focus will therefore centre on banks' financial resilience including the adequacy of capital and liquidity buffers, the robustness of stress testing and scenario analysis capabilities , and the integration of market risk forward-looking strategic decision making.
5. Fraud, scams evolving financial crime risk	Financial crime risks remain elevated, with the CBI highlighting a continued increase in fraud and scam activity, driven by digitalisation, cross-border complexity and the growing use of advanced technologies. Supervisory activity will focus on strengthening firms' AML/CFT frameworks, enhancing fraud detection and response capabilities, and ensuring appropriate customer protection where incidents occur. This includes targeted reviews of fraud controls, increased data collection (including AML/CFT REQs), and ongoing scrutiny of firms' ability to adapt to evolving financial crime typologies.

How we can help



Operational and cyber resilience / DORA

Our client-selectable services include:

- DORA implementation reviews (ICT governance, cyber risk, outsourcing).
- Critical/Important Business Services (CIBS) mapping validation.
- Threat Led Penetration Testing (TLPT) readiness.
- Cloud/third party dependency and exit strategy assessments.
- Operational resilience scenario testing & board reporting enhancement.

AML, fraud and financial crime

Our client-selectable services include:

- Enhanced AML/CFT REQ data quality reviews.
- AML/CFT framework effectiveness assessment.
- Fraud risk uplift with AI enabled detection capabilities.
- KYC/EDD and sanctions-screening effectiveness reviews.

Data quality, RDARR and AI / model risk governance

Our client-selectable services include:

- RDARR remediation and data governance uplift Complaints-handling diagnostic and root cause remediation.
- Model risk governance aligned to EU AI Act (explainability, bias testing).
- Validation of credit, market, pricing and fraud detection models.
- Data lineage and regulatory reporting accuracy testing.

Financial risk, credit, liquidity and climate

Our client-selectable services include:

- SREP-aligned assessments (credit, liquidity, climate, market risk).
- Mortgage and short-term lending vulnerability diagnostics.
- Climate risk integration into credit, collateral valuation and capital planning.
- ICAAP/ILAAP enhancement and stress testing support.

Consumer Protection and CPC 2026

Our client-selectable services include:

- CPC 2026 readiness assessments across product governance, digital journeys and disclosures.
- Complaints-handling diagnostic and root cause remediation.
- Vulnerable customer framework review.
- Testing of app-based sales and digital communications.

Governance, board oversight and accountability (IAF/SEAR)

Our client-selectable services include:

- Board and committee effectiveness reviews (focus on tech, cyber, outsourcing, climate) Digital and offline communication pathways.
- SEAR/IAF implementation reviews (responsibility maps, reasonable steps) Fraud response and customer notification processes.
- Risk appetite and policy alignment to CBI expectations.

Supervisory engagement and inspection readiness

Our client-selectable services include:

- Mock CBI inspections (DORA, CPC, AML, conduct, climate, outsourcing) AML/CFT framework effectiveness assessment.
- Pre submission review of supervisory engagement packs.
- Remediation planning for previous CBI findings.

The RSM team

Colm Laird
Partner, Risk and Governance
colm.laird@rsmireland.ie

Michael Mulholland
Head of Audit, Financial Services Leader
mmulholland@rsmireland.ie

Ian McCartney
Director, Risk and Governance
ian.mccartney@rsmuk.com

Divan Steyn
Senior Manager, Risk and Governance
divan.steyn@rsmireland.ie

Ann Marie Conroy
Senior Manager, Risk and Governance
annmarie.conroy@rsmireland.ie

Sive Riznyczok
Manager, Risk and Governance
sive.riznyczok@rsmireland.ie

Yevgen Shuvalov
Consultant, Risk and Governance
yshuvalov@rsmireland.ie

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM Ireland

Block D, Iveagh Court,
Harcourt Rd,
Dublin 2,
D02 VH94
T +353 (0)1 496 5388
www.rsmireland.ie