CBI Supervisory Outlook 2026

Payments and E-Money sector



THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

Payments and E-Money 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 Payments and E-Money sector specific considerations for 2026:

- The payments and e-money sector has grown rapidly, now representing a critical component of the European payments landscape. Yet this sector is also one of the most vulnerable from a regulatory and operational risk standpoint. The CBI identifies ongoing weaknesses in safeguarding, financial crime controls, governance, and operational resilience that warrant sustained and intensive supervision throughout 2026.

- The most pressing issue remains the **safeguarding of customer funds**. Because these firms' client balances do not benefit from a deposit guarantee scheme, failures in safeguarding frameworks can result in severe consumer harm. The CBI has conducted extensive inspections and audits over recent years, but significant deficiencies persist. As a result, the regulator has introduced a new Pre-Approved Controlled Function—the Head of Safeguarding—to strengthen accountability and expects all firms to remediate weaknesses promptly and comprehensively.

- The sector is also experiencing a sharp rise in **fraud and financial crime**, with fraudulent transactions among Irish payment and e-money firms tripling to €57m in 2024. AI enabled scams, cross border money laundering typologies, and rapid onboarding processes compound the risk. The CBI will rely on an enhanced AML/CFT Risk Evaluation Questionnaire, targeted inspections, and increased expectations for data quality, monitoring systems and customer support in fraud cases.

- Operational and cyber resilience is another central focus, particularly as the sector continues to suffer from significant system outages and disruption events, some of which have affected the broader payments ecosystem. Firms must demonstrate strong IT outsourcing oversight, DORA implementation, incident classification and reporting, and credible recovery capabilities.

- **Business model sustainability and wind down planning** represent additional areas of regulatory concern. Many payments firms face challenges achieving sustainable profitability, which increases the risk of disorderly exits. The CBI expects wind down plans to be actionable, prioritise the timely return of customer funds, and consider practical obstacles to resolution.

- Finally, there are persistent concerns about **governance and culture**. The CBI has observed instances of weak customer centricity, slow remediation of identified issues, poor root cause analysis and inadequate treatment of vulnerable customers. With PSD3 and the new Payment Services Regulation approaching, firms must strengthen their risk management, governance frameworks and operational readiness.



Key 2026 supervision themes

Upcoming regulatory changes - The CBI has also placed additional focus on the new upcoming regulatory changes regarding PSD3 / Payment Services Regulation (PSR), DORA full implementation, Access to Cash, and regulatory responsibilities.

Safeguarding of customer funds - Persistent weaknesses remain despite extensive prior supervisory action. The CBI expects strengthened safeguarding processes, a Head of Safeguarding PCF responsibility (effective February 2026), and continuous review of segregation, reconciliations and safeguarding accounts.

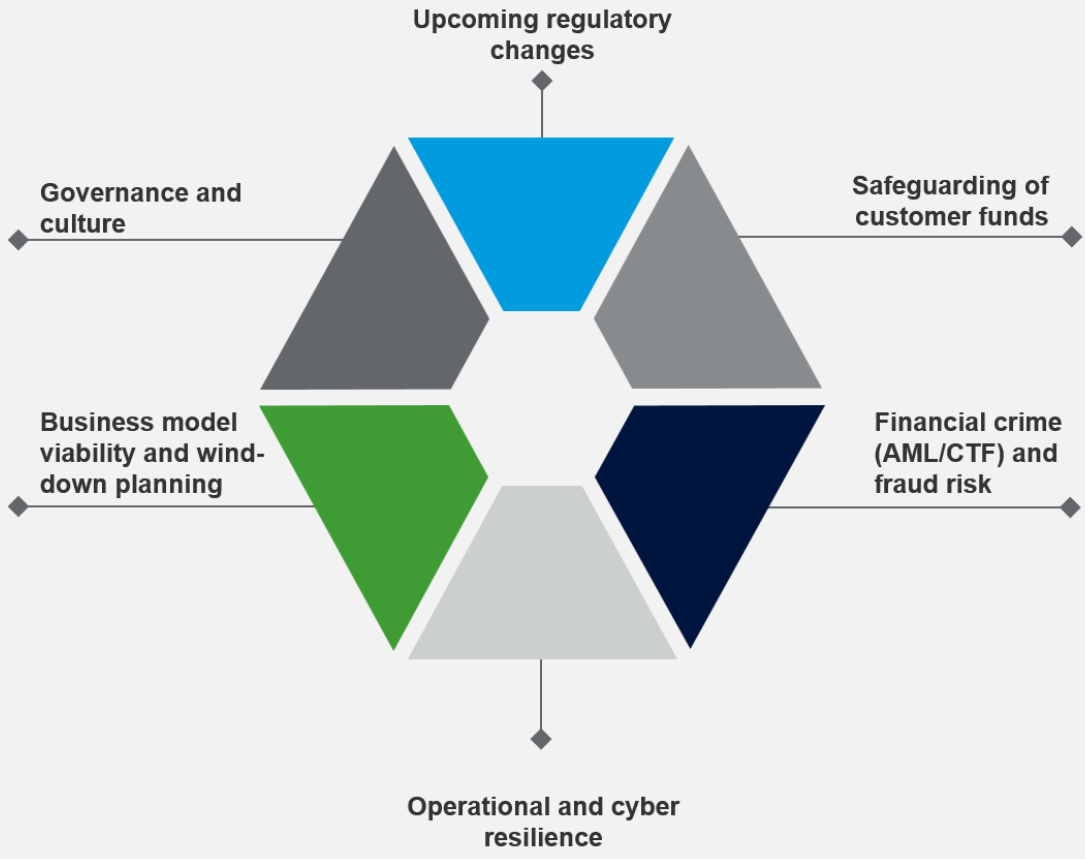
Financial crime (AML/CTF) and fraud risk - Payments/e-money firms are extremely exposed due to high volumes of transactions, cross-border flow and digital models. The CBI highlights €57m fraud reported in 2024 (a threefold increase), growing AI-driven scams and persistent AML control weaknesses. Supervisory focus includes enhanced AML requirements, inspections and thematic reviews, and fraud controls and customer remediation.

Operational and cyber resilience - The CBI notes a high dependency on IT outsourcing as well as third-party providers in this sector. The CBI is completing thematic reviews and DORA monitoring on outsourcing governance, major incident reporting, cloud dependency, and system outage response.

Business model viability and wind-down planning - Many firms struggle for profitability; however, the CBI requires failures to be orderly. The CBI will scrutinise wind-down triggers and customer money return processes, strategic planning and financial resilience, and the impact of the EBA's updated definition of e-money.

Governance and culture - The CBI has observed problems which warrant heightened supervision, including weak customer-centric culture, poor complaints handling, and inadequate board oversight. The CBI will conduct reviews across vulnerable customers, board composition, and agent/distributor oversight.

Figure 1: Key 2026 supervisory themes



RSM assessment: heat map of key regulatory and supervisory risks in the Payments and E-Money sector

Key risk area of focus for 2026	Severity	Rational behind the 2026 key focus risk areas	Further consideration
Safeguarding of customer funds	Severe	Customer funds are not protected by deposit guarantee schemes. Any safeguarding failure directly exposes customers to total loss.	The CBI continues to report persistent deficiencies in safeguarding controls and had to introduce a new Head of Safeguarding PCF due to repeated issues. This is considered one of the most critical risks in the sector.
Financial crime (AML/CTF) and fraud risk	Severe	Payment firms process high transaction volumes at high speed, making them prime channels for scams, mule accounts and money laundering.	Fraud among Irish payment and e-money firms tripled to €57m in 2024. AI driven scams and AML framework weaknesses heighten risk. The CBI receives high levels of whistleblowing disclosures.
Operational and cyber resilience	Severe	The sector has experienced significant outages affecting merchants and consumers. Heavy outsourcing raises dependency and concentration risk.	The CBI notes cross industry outages, weak IT outsourcing oversight, and the need for improved DORA reporting. Failures could disrupt national payments infrastructure.
Business model viability and wind-down planning	High	Many firms struggle for profitability; failure is likely without adequate capital and wind down plans. Poor planning could leave customers stranded.	The CBI reports insufficient wind down triggers, unclear customer fund return processes, and concerns about consolidation risks. Some firms depend on parent funding.
Consumer protection and governance	High	Weak customer centric cultures increase risk of service failures, poor dispute resolution and recurring errors.	The CBI observed poor complaints handling, inadequate treatment of vulnerable customers, and weak governance structures. Culture seems to be a recurring problem.
Regulatory change readiness	Moderate	Firms must prepare for multiple regulatory changes in parallel—PSD3, the new PSR, and full DORA compliance.	Many firms are behind in implementing DORA. PSD3 and the PSR introduce new obligations and scrutiny that firms must prepare for before 2028.

Severity ratings represent RSM's interpretation of the relative supervisory and control risk based on the Central Bank's 2026 Regulatory & Supervisory Outlook and related MiCAR supervisory priorities. They are not CBI-assigned risk ratings.

What the CBI's 2026 outlook means for the Payments and E-Money sector

The Central Bank of Ireland's 2026 Regulatory & Supervisory Outlook sends its strongest signal to date that **the payments and e money sector will face intensified supervisory scrutiny throughout 2026**. The CBI describes the sector as both fast growing and high risk, highlighting repeated issues across safeguarding, operational resilience, financial crime, data quality and governance. As such several strategic implications arise for Boards and executive teams:



The CBI considers the sector to have persistent structural weaknesses

Despite years of inspections, thematic reviews and remediation cycles, the CBI continues to find **significant deficiencies in safeguarding frameworks**, including reconciliations, segregation of funds, and governance oversight. This led to the creation of a new PCF role—Head of Safeguarding which is effective from February 2026. Companies should make sure that this new requirement is filled ASAP If not already.



Payments firms are now seen as high risk vectors for fraud and financial crime

Fraud losses tripled to €57 million in 2024 among Irish payment and e money firms, driven by AI enabled scams, mule account activity and weaknesses in AML systems. The CBI is responding with enhanced AML/CFT risk evaluation questionnaires (REQs), targeted inspections and an expectation of significantly improved data quality and monitoring capabilities.



Operational outages pose systemic risk in a digital first payments ecosystem

The CBI notes repeated industry wide system outages, often linked to weak oversight of outsourced or cloud based providers, and has elevated **DORA compliance** as a core supervisory priority. Payments firms must demonstrate credible third party dependency mapping, cyber resilience, and robust incident classification and reporting processes.

What the CBI's 2026 outlook means for the Payments and E-Money sector (Cntd.)

Business model fragility is now treated as a consumer protection risk

Many EMIs and PSPs still struggle to reach sustainable profitability. The CBI fears disorderly firm exits could leave customers stranded or without timely access to funds. Supervisors will scrutinise wind down triggers, fund return processes, and capital/liquidity planning throughout 2026.

Culture and governance shortcomings remain common

The CBI continues to observe poor complaints handling, weak treatment of vulnerable customers, slow remediation of identified issues, and board structures that lack the expertise to oversee safeguarding, outsourcing and financial crime. This area will be a major focus in 2026.

In short: The CBI expects payments and e money firms to move from aspirational compliance to evidenced capability, especially in safeguarding, operational resilience and fraud prevention



RSM recommended focus areas for Payment and E-Money companies to take in 2026 (Q2–Q4 priority roadmap)

Safeguarding: act now (highest priority)	▪ Conduct a full safeguarding framework review, including account structures, reconciliations and daily safeguarding calculations. ▪ Confirm the Head of Safeguarding (PCF) appointment and ensure reporting lines to the Board are functioning. ▪ Undertake a mock safeguarding inspection to test governance, evidence, and documentation.
AML/CFT and fraud controls: strengthen data and monitoring	▪ Prepare the enhanced AML/CFT REQ with improved data governance, transaction monitoring accuracy and sanctions screening. ▪ Upgrade fraud frameworks to address AI enabled scams, cross border typologies, and rapid onboarding risks. ▪ Conduct a review of customer remediation practices for fraud victims.
DORA and operational resilience: implement core controls by mid-2026	▪ Finalise CIBS mapping and impact tolerances. ▪ Validate major incident reporting processes under DORA. ▪ Map critical dependencies on cloud and outsourced providers and develop credible exit strategies. ▪ Perform scenario based operational resilience tests simulating system outages.
Business model and wind down readiness: ensure credibility	▪ Review and strengthen wind down triggers, governance and communication plans. ▪ Test end to end customer fund return processes to ensure speed, accuracy and auditability. ▪ Conduct profitability stress tests, especially for fast scaling or cross border firms.
Governance and culture: uplift board readiness	▪ Enhance Board reporting on safeguarding, AML, outsourcing, complaints and vulnerabilities. ▪ Strengthen oversight of distributors, agents and white label partners. ▪ Conduct a governance and Senior Executive Accountability Regime (SEAR)/Individual Accountability Framework (IAF) alignment review
PSD3 / PSR: begin gap analysis in 2026	▪ Assess changes to fraud liability, consumer disclosures, transparency obligations and Strong consumer Authentication (SCA) requirements. ▪ Identify operational and system changes required ahead of 2028 implementation timelines.

Areas of expected supervisory intensification in 2026



Area	Rational behind the 2026 key focus risk areas
1. Safeguarding failures (zero tolerance area)	Safeguarding is the CBI's top payment sector risk. Years of recurring deficiencies mean firms should expect: • repeat inspections • deep dives into reconciliation and segregation processes • reviews of governance and Board oversight evidence.
2. Fraud management and AML weaknesses	Fraud tripled year on year and is now seen as a systemic risk. Inspections are likely to focus on: • AI driven scam detection • transaction monitoring tuning • customer handling after fraud events • Whistleblower disclosures and incident reporting
3. Outsourcing and cloud dependency risks	System outages across multiple payment firms in 2025 have elevated concerns. Expect scrutiny of: • cloud concentration risk • sub outsourcing chains • exit strategies and dependency mapping • DORA "register of information" accuracy
4. Business model viability and wind down execution	Firms with weak profitability or reliance on parent funding will be prioritised. Supervisors will assess: • realism of wind down triggers • customer fund return readiness • capital resilience during stress
5. Culture, governance and customer outcomes	The CBI has repeatedly found that poor culture leads directly to customer harm. Expect: • thematic reviews on complaints handling • assessments of vulnerable customer frameworks • governance deep dives where repeated issues persist
6. Regulatory change readiness (PSD3 / PSR / DORA)	Firms behind on DORA or not yet preparing for PSD3/PSR can expect intrusive engagement, including data requests, desk based reviews and follow up visits.

How we can help



Safeguarding Framework Strengthening

Our client-selectable services include:

- Full safeguarding framework assessment (structures, reconciliations, segregation, daily calculations).
- Independent review of Head of Safeguarding PCF role and governance reporting.
- Testing of safeguarding controls, evidence packs, and remediation tracking.
- Oversight reviews of agents, distributors, and third party reliance in safeguarding chains.



AML, CFT and fraud risk enhancement

Our client-selectable services include:

- Enhanced AML/CFT REQ preparation & data quality validation.
- AML framework review: KYC, EDD, sanctions screening, governance.
- Fraud risk assessment including AI enabled scams, onboarding risks & transaction monitoring tuning.
- Customer remediation review following fraud events (a major CBI theme).



Operational resilience and DORA compliance

Our client-selectable services include:

- DORA readiness review (ICT governance, incident reporting, outsourcing).
- Testing of “Register of Information” and major incident reporting processes.
- Cloud and third party dependency mapping and credible exit strategies.
- Scenario based resilience testing and CIBS mapping validation.



Business model viability and wind down planning

Our client-selectable services include:

- Independent wind down plan reviews covering triggers, governance and fund return readiness.
- End to end customer fund return process testing.
- Capital, liquidity and profitability stress testing for EMIs/PSPs.



Governance, culture and customer outcomes

Our client-selectable services include:

- Board governance reviews (safeguarding, AML, outsourcing, customer outcomes).
- SEAR/IAF implementation reviews (responsibility maps, reasonable steps).
- Customer outcomes and complaints handling assessments aligned to CBI expectations.
- Vulnerable customer and agent/distributor oversight reviews.



PSD3 / PSR and regulatory change readiness

Our client-selectable services include:

- Gap analysis for PSD3 and PSR reforms (fraud liability, SCA, disclosures, transparency).
- Operational change impact assessments for 2028 implementation.
- Review of open banking API risks and strong customer authentication controls.

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

RSM Ireland is a member of the RSM Network and trades as RSM. RSM is the trading name used by the members of the RSM Network. Each member of the RSM Network is an independent assurance, tax and consulting firm each of which practices in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction.

The network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 200 Aldersgate Street, Upper Ground Floor South, London, EC1A 4HD. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

© RSM Ireland, 2026