RSM

CBI Supervisory Outlook 2026

Crypto sector

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

Crypto 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.

The Outlook links these developments to the Central Bank's supervisory focus on resilience, consumer and investor protection, financial-system integrity and effective risk management.

2

Operational and cyber risks remain prominent cross-sector supervisory concern, driven by digitalisation, complexity, outsourcing and geopolitical risk.

The 2026 Outlook also highlights consumer and investor protection, financial crime, technology-driven transformation including AI, and environmental and societal transitions as important supervisory themes.

Introduction

What follows are the crypto specific considerations for 2026:

- **Markets in Crypto Assets Regulation (MiCAR)** has brought crypto-asset service providers within a new EU regulatory framework, creating a significant new area of authorisation and supervision for the Central Bank of Ireland. MiCAR became applicable to Crypto-Asset Service Providers (CASPs) on 30 December 2024, bringing in-scope crypto-asset services within a harmonised **EU regulatory framework.** The CBI identifies heightened consumer and investor risk in crypto, reflecting the volatile and inherently high-risk nature of crypto-assets, complex CASP business models, and technical challenges such as private key security. Financial crime should also remain a key control focus for CASPs given the wider AML/CFT obligations applicable to regulated firms. The notification and publication of MiCAR Title II white papers is now an important supervisory data point under the MiCAR framework.

- A key supervisory focus is operational resilience and safeguarding risk, including technical challenges such as private key security and custody arrangements. Weakness in private key governance or custody controls could create **material operational and consumer risk.** Firms should therefore expect supervisory scrutiny of controls, segregation practices and authorisation conditions imposed during licensing. Operational and cyber resilience is another critical risk area. CASPs must demonstrate compliance with DORA, and the sector will be subject to an ESMA led Common Supervisory Action on cyber risk. This reflects the expectation that CASPs subject to DORA must evidence robust operational resilience frameworks appropriate to the services they provide.

- **Financial crime risk**, including AML/CFT compliance, remains a key supervisory and control consideration for CASPs. Crypto environments present unique typologies due to pseudonymous transactions, cross border flows, and rapid account opening. CASPs should expect AML/CFT frameworks, data quality, transaction monitoring and sanctions screening to remain areas of supervisory and internal- control focus.

- Finally, **consumer protection** sits at the centre of the CBI's approach. CASPs must ensure transparent disclosures, fair marketing, suitability controls, and robust governance. The CBI's focus on treatment of customers means CASPs should be able to evidence clear disclosures, appropriate product governance and controls to mitigate consumer and investor detriment. Overall, supervisors expect CASPs to mature quickly, embedding governance, resilience and integrity standards comparable to the rest of the financial sector.

Key 2026 supervision themes

Consumer protection and risk - The CBI identifies heightened consumer and investor detriment risk in crypto, including risks arising from volatility, complex CASP business models, sophisticated products, poor or opaque disclosures and product unsuitability.

Operational and cyber resilience - The CBI's planned activities include targeted work on CASPs in relation to DORA compliance, alongside ESMA thematic work on cyber risk as part of a wider Common Supervisory Action on the CASP sector.

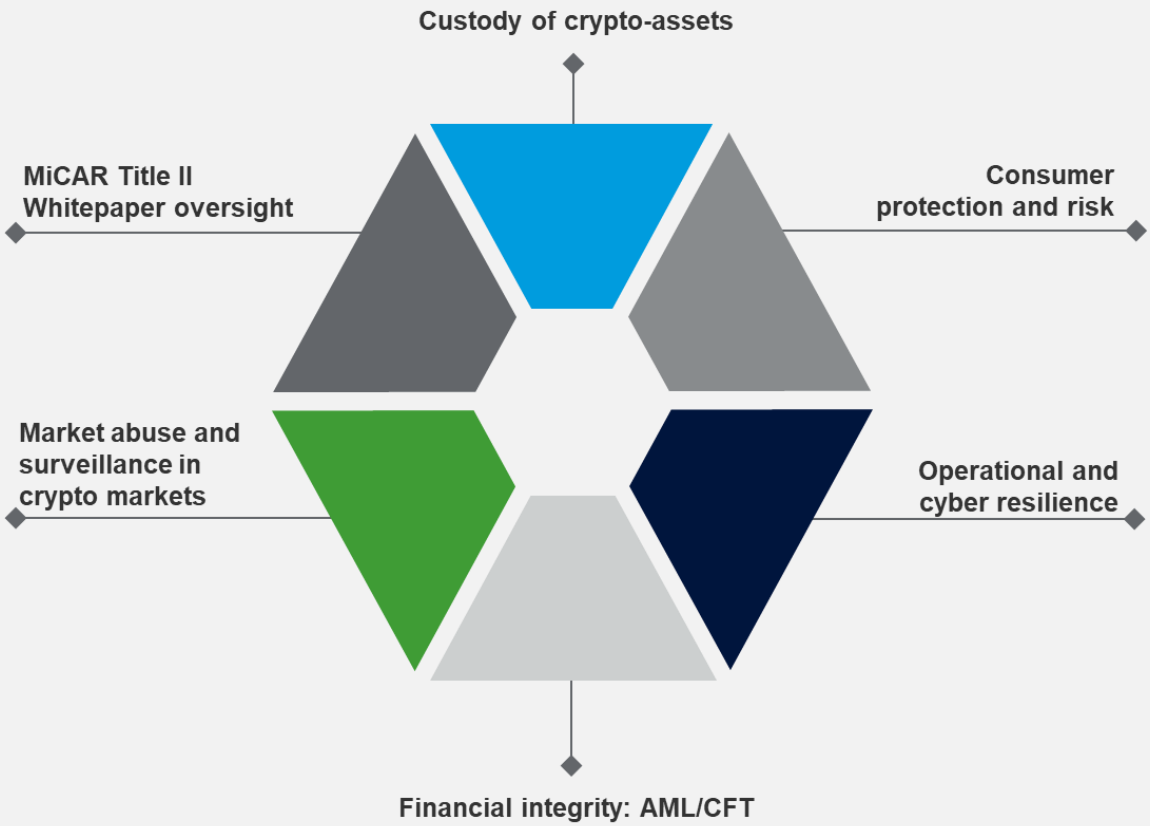
Financial integrity: AML/CFT - Given the nature of crypto-asset activity, CASPs should ensure AML/CFT risk assessments, customer due diligence, transaction monitoring and sanctions controls are robust, current and capable of evidencing compliance.

Market abuse and surveillance in crypto markets - MiCAR introduces market abuse obligations for in-scope crypto-asset activity, including suspicious transaction and order reporting. CASPs should therefore ensure that surveillance and escalation arrangements are robust

MiCAR Title II Whitepaper oversight - MiCAR Title II white paper requirements are now in force for crypto-assets other than ARTs and EMTs, and firms should ensure that white paper disclosures are complete, accurate and consistent with MiCAR requirements.

Custody of crypto-assets - The CBI has highlighted private key security as a distinct technical challenge in CASP business models. As a result, custody governance, segregation and safeguarding controls should be treated as priority control areas.

Figure 1: Key 2026 supervisory themes



RSM assessment: heat map of key regulatory and supervisory risks in the crypto sector

Key risk area of focus for 2026	Severity	Rationale behind the 2026 key focus risk areas	Further consideration
Client asset safeguarding / custody	Severe	Loss, theft or unauthorised transfer of crypto-assets can be difficult or impossible to reverse and may cause significant customer harm.	The CBI highlighted private key security as a distinct technical challenge in CASP business models. Crypto custody is inherently high risk, and MiCAR imposes strict safeguarding rules that firms are still maturing into.
Financial Crime / AML	Severe	Crypto's pseudonymous and cross border nature attracts sophisticated money laundering and terrorist financing activity. CASPs should be able to evidence mature, risk-based AML/CFT frameworks appropriate to their business model and risk profile.	CASPs often face fast customer onboarding, complex flows, and limited visibility of beneficial owners. Given evolving financial crime typologies, CASPs should keep transaction monitoring, sanctions screening and investigation processes under regular review Enhanced AML REQs and supervisory engagement are likely to focus on compliance.
Consumer protection	Severe	Retail consumers may not understand the risks of highly volatile, complex or novel crypto products. Where governance or disclosure practices are not sufficiently mature, CASPs may expose consumers and investors to heightened detriment risk	The CBI cites clear risks: volatile pricing, opaque business models, insufficient disclosures, and high retail exposure. Weak suitability frameworks create risks of mis selling or financial loss.
Operational and cyber resilience	High	CASPs depend heavily on cloud infrastructure, APIs, and digital wallets. Outages or cyber breaches can immediately compromise assets and client access.	ESMA thematic work on cyber risk is planned as part of a wider Common Supervisory Action on the newly established CASP sector. The CBI stresses that CASPs must meet DORA standards despite being new entrants. Many firms rely on untested or immature operating environments.
Market integrity / surveillance	High	Crypto markets are vulnerable to manipulation (wash trading, spoofing, pump and dump) due to fragmented venues and low transparency.	CASPs should ensure that market abuse surveillance and suspicious transaction and order reporting arrangements are effective and appropriately documented. Regulation is ahead of capability in many firms.
Governance and culture	High	Many CASPs are young firms with limited regulatory history. Boards may lack financial-services maturity, leading to weak oversight.	As CASPs move into the MiCAR supervisory framework, governance, control frameworks and risk management arrangements will need to be capable of demonstrating compliance with regulatory expectations. Some firms require significant uplift to meet minimum expectations.

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

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

With MiCAR applicable to CASPs from 30 December 2024, **2026, is an important year for CASPs to evidence how they are meeting their regulatory obligations in practice**.

RSM view: CASPs will need to evidence mature governance, control and resilience arrangements under MiCAR and DORA

For many CASPs, MiCAR represents a step-change in regulatory expectations and supervisory engagement. CASPs are likely to face challenges in developing consistent governance frameworks, effective internal controls and sufficient Board-level financial services risk expertise. CASPs should uplift governance and internal controls to meet the requirements and supervisory expectations applicable under MiCAR, DORA and relevant AML/CFT obligations."

MiCAR white paper volumes mean deeper supervisory scrutiny

MiCAR white paper requirements increase the importance of accurate, complete and clear disclosures for in-scope crypto-assets. Firms should ensure white paper disclosures, risk explanations, conflicts disclosures and product-governance arrangements are accurate, complete and capable of review.

Financial integrity, cyber resilience, and consumer protection are priority risks

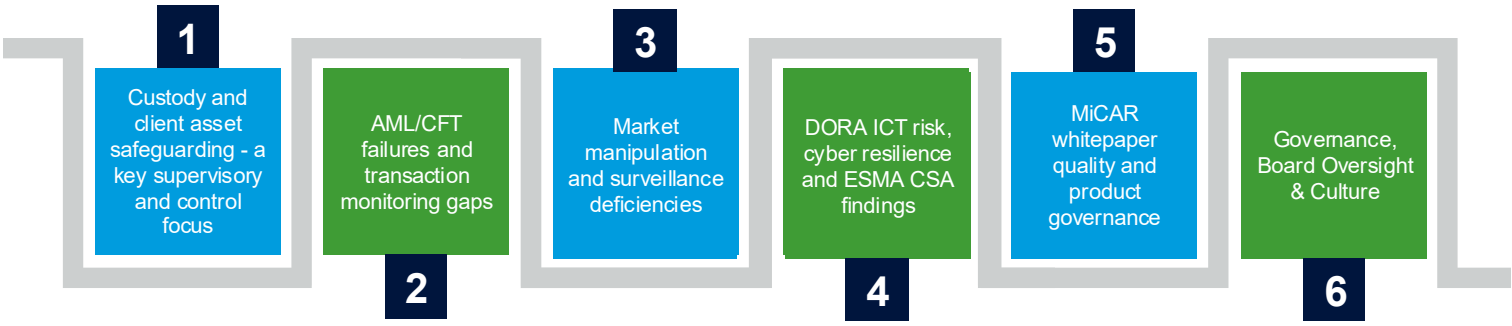
Because crypto environments are pseudonymous, borderless, and technology dependent, the CBI considers CASPs to be high risk for AML/CFT breaches, fraud, misconduct, cyberattacks, and market manipulation. Supervisors will use enhanced data collection, targeted inspections, and an ESMA led cyber - Common Supervisory Action to test firms' resilience and compliance.

In essence: 2026 is the year CASPs are expected to demonstrate institution level governance, transparent disclosures, robust custody frameworks, and operational resilience equivalent to traditional regulated entities.

RSM recommended focus areas for CASPs in 2026 (Q3 - Q4 priority roadmap)

Strengthen custody and private key governance	▪ Conduct independent reviews of custody arrangements, including private key management, multisig controls, wallet segregation and cold storage governance. ▪ Test loss of key and wallet compromise contingencies and document recovery procedures. ▪ Confirm compliance with MiCAR custody requirements and CBI expectations for segregation of client vs. firm assets.
Enhance AML / CFT and financial integrity controls	▪ Prepare for the enhanced AML/CFT REQ, ensuring data quality, typology mapping, and monitoring completeness ▪ Consider whether blockchain analytics and typology-based monitoring are appropriate and proportionate to the firm's risk profile. ▪ Strengthen onboarding, KYC and EDD procedures.
Deliver DORA operational resilience compliance	• Identify critical or important functions, ICT dependencies and third-party arrangements supporting crypto-asset services. ▪ Assess third party dependencies (cloud services, wallet providers, chain analytics vendors). ▪ Conduct cyber resilience testing aligned to the ESMA led CSA on crypto cyber risk.
Strengthen consumer protection and fair marketing controls	▪ Review whitepaper disclosures, volatility warnings, liquidity risk statements, fork/suspension risks. ▪ Implement robust marketing review procedures, especially for retail products. ▪ Review product governance, appropriateness/suitability processes where applicable, and customer risk disclosures for complex, high-risk or illiquid crypto products
Improve market integrity and surveillance frameworks	▪ Validate STOR (Suspicious Transaction & Order Report) processes for crypto markets. ▪ Upgrade surveillance systems to detect wash trading, spoofing, layering, cross market manipulation, pump and dump patterns, and on chain abuse. ▪ Strengthen token listing governance, including conflict of interest controls.
Uplift governance, board capability and accountability	▪ Conduct governance maturity reviews, particularly around risk, cyber, AML and custody oversight. ▪ Consider accountability mapping and governance responsibilities under applicable SEAR/IAF requirements. ▪ Provide Board training on MiCAR, DORA, cyber risks, and crypto-market integrity obligations.

Areas of expected supervisory intensification in 2026



Area	Rationale behind the 2026 key focus risk areas
1. Custody and client asset safeguarding (top supervisory priority)	Crypto custody failures - private key loss, wallet compromise, commingling of firm and client assets - pose irreversible consumer harm. Firms should be prepared to evidence: ▪ private key governance ▪ wallet segregation ▪ third party custody oversight ▪ Incident response arrangements
2. AML/CFT failures and transaction monitoring gaps	Potential focus areas for firm self-assessment include: ▪ transaction monitoring ▪ sanctions screening ▪ customers due diligence ▪ enhanced due diligence and data quality
3. Market manipulation and surveillance deficiencies	MiCAR introduces a market abuse framework for crypto-assets, including obligations relating to suspicious transaction and order reporting. CASPs should ensure that surveillance, escalation and governance arrangements are appropriate to their services and trading activity
4. DORA ICT risk, cyber resilience and ESMA CSA findings	CASPs should expect supervisory focus on: ▪ DORA compliance ▪ Operational resilience maturity ▪ Cyber-risk management
5. MiCAR whitepaper quality and product governance	Firms should ensure white paper disclosures clearly address: ▪ material risks ▪ token features ▪ conflicts of interest ▪ relevant product-governance considerations
6. Governance, board oversight and culture	Boards and senior management should be able to evidence: ▪ appropriate oversight of crypto-specific risks ▪ effective challenge of management decisions ▪ clear accountability and governance structures ▪ sufficient governance maturity relative to business model

How we can help

Custody and client asset safeguarding

Our client-selectable services include:

- Independent review of private key management, multi-signature controls, wallet segregation and cold storage governance.
- Testing of key loss recovery procedures and custody incident readiness.
- Assessment of Markets in Crypto Assets Regulation (MiCAR) custody compliance and segregation of client vs. firm assets.
- Oversight review of third-party custody/wallet technology providers.

Operational resilience and DORA compliance

Our client-selectable services include:

- DORA aligned ICT, cyber, incident management and recovery assessments.
- Identification of critical or important functions, ICT dependencies and third-party arrangements supporting crypto-asset services.
- Testing of cloud, protocol and API dependencies.
- Support for European Securities and Markets Authority (ESMA) led cyber-common Supervisory Action (CSA) expectations.

Consumer protection, disclosures and conduct

Our client-selectable services include:

- Review of MiCAR whitepaper disclosures and risk warnings (volatility, liquidity, forks, suspension risks).
- Marketing and promotions compliance reviews (retail focus).
- Suitability framework testing for complex or leveraged products.
- Assessment of onboarding journeys and complaint handling standards.

AML/CFT and financial integrity controls

Our client-selectable services include:

- Enhanced AML/CFT Risk Evaluation Questionnaire (REQ) preparation and data quality checks.
- Blockchain analytics assessments (cross chain flows, mixer/tumbler exposure, sanctions tracing).
- Review of transaction monitoring for pseudonymous environments.
- Strengthening onboarding, KYC and Enhanced Due Diligence (EDD) processes.

Market integrity and surveillance

Our client-selectable services include:

- Review of the Suspicious Transaction and Order Report (STOR) frameworks for crypto markets.
- Validation of market surveillance tooling (wash trading, spoofing, layering, pump and dump, on chain manipulation).
- Assessment of token listing governance and conflict of interest controls.

Governance, board capability and accountability

Our client-selectable services include:

- Governance effectiveness reviews focused on custody, market integrity, AML and operational resilience.
- SEAR/IAF mapping for crypto leadership roles (Head of Custody, CTO, Money Laundering Reporting Officer - MLRO).
- Board training on MiCAR, DORA, crypto risk typologies and CBI supervisory expectations.

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