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.

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 crypto specific considerations for 2026:

- The newly regulated crypto-asset sector represents one of the most significant areas of supervisory expansion for the CBI. As Markets in Crypto Assets Regulation (MiCAR) came into force, Crypto Asset Service Providers (CASPs) entered the regulatory perimeter, many for the first time. Given the sector's high retail participation, complex market structures, reliance on novel technologies and cross border nature, the CBI views the crypto domain as carrying **elevated consumer, operational and financial crime risks.** This is reflected in the volume of activity already underway: in 2025 alone, over **300 MiCAR Title II whitepapers** were notified to the Central Bank, far exceeding expectations and demonstrating the speed at which the sector is innovating.

- A central supervisory priority is **client asset safeguarding**, particularly the security of private keys and the robustness of custody arrangements. Mismanagement or cyber compromise of these keys could lead to significant customer harm, and the CBI is applying close scrutiny to firms' 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 CBI's expectation that crypto firms must match the resilience standards applied to traditional financial entities, despite their comparatively recent entry into regulation.

- **Financial integrity risk**—including AML/CFT compliance—remains one of the highest concerns. Crypto environments present unique typologies due to pseudonymous transactions, cross border flows, and rapid account opening. The CBI will deploy enhanced AML data collection, targeted supervisory engagement, and deeper reviews of transaction monitoring systems throughout 2026.

- 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 has stated it will intervene early and assertively where firms fail to demonstrate that customers understand the risks of the crypto products they consume. 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 - CASPs have large retail customer bases and complex, high-risk products. The CBI will scrutinize their disclosure quality, product suitability, marketing practices, and governance and board oversight for early engagement before launching new services.

Operational and cyber resilience - CASPs must comply with DORA. As such, the CBI is focusing on conducting cyber risk assessments, DORA compliance testing, and ESMA-led Common Supervisory Action (CSA) on cyber risk for CASPs.

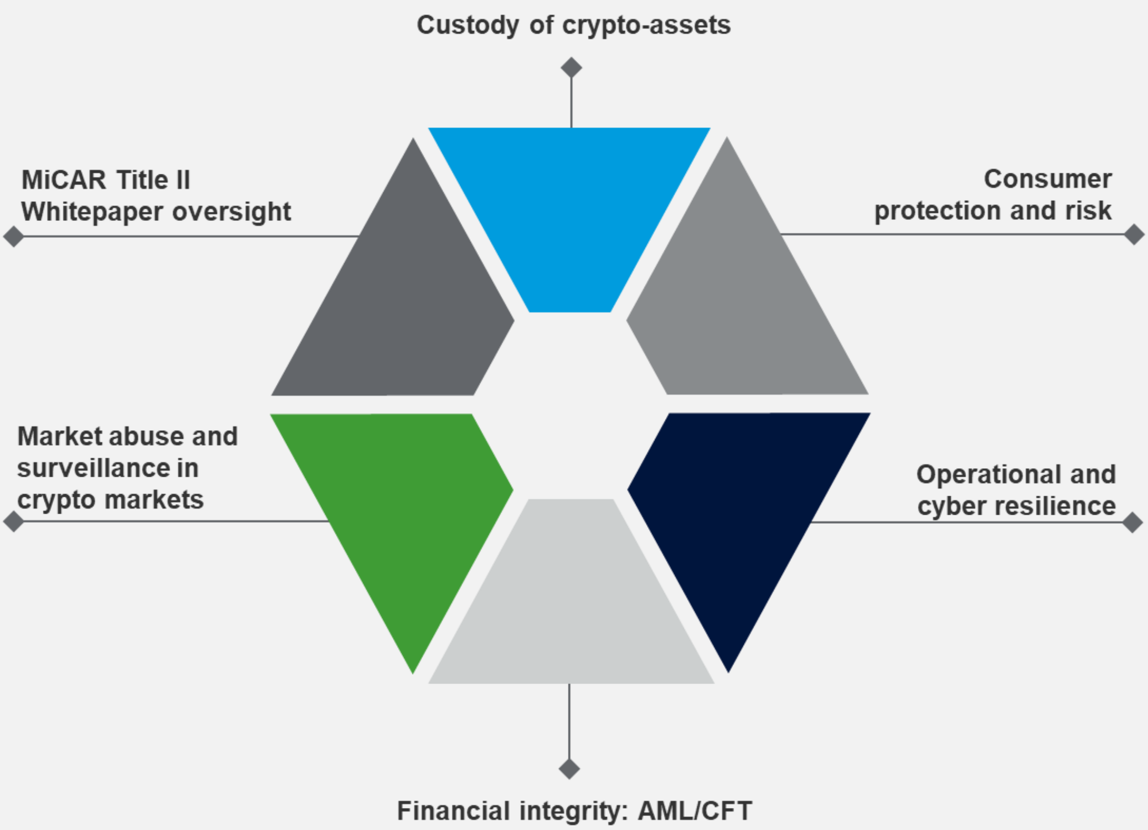
Financial integrity: AML/CFT - Crypto's cross border pseudonymous nature raises significant ML/TF risk. As such, the CBI will specifically focus on overseeing enhanced AML REQ (data collection), targeted AML inspections, transaction monitoring effectiveness, and sanctions screening.

Market abuse and surveillance in crypto markets - Given the high level of risk attributed to this sector, the CBI will specifically focus on monitoring the Crypto Asset Service Providers' detection of manipulative trading, STOR reporting, and surveillance controls.

MiCAR Title II Whitepaper oversight - The CBI received 300+ whitepapers in 2025 and will because of that intensify its scrutiny of disclosure accuracy and risk explanations in 2026 and going forward.

Custody of crypto-assets - Custody of crypto-assets is considered to be a high-risk area due to private key compromise, hacking and safekeeping failures. The CBI will conduct follow-up examinations on segregation of client assets, safeguarding controls, and implementation of MiCAR custody requirements.

Figure 1: Key 2026 supervisory themes



Heat map of key regulatory and supervisory risks in the crypto sector

Key risk area of focus for 2026	Severity	Rational behind the 2026 key focus risk areas	Further consideration
Client asset safeguarding / custody	Severe	Loss or theft of crypto-assets is irreversible. Private key mismanagement, hacks, or commingling of client assets can cause catastrophic consumer harm.	The CBI highlights persistent weaknesses in custody models and private key controls. 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. Many CASPs lack mature AML frameworks.	CASPs often face fast customer onboarding, complex flows, and limited visibility of beneficial owners. The CBI notes AML typologies evolving faster than controls. Enhanced AML REQs and inspections will test compliance.
Consumer protection	Severe	Retail consumers may not understand the risks of highly volatile, complex or novel crypto products. Many CASPs have immature governance and weak disclosure practices.	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 has launched a sector wide cyber CSA due to elevated concerns. The CBI stresses that CASPs must meet DORA standards despite being new entrants. Many firms rely on untested or immature operational environments.
Market integrity / surveillance	High	Crypto markets are vulnerable to manipulation (wash trading, spoofing, pump and dump) due to fragmented venues and low transparency.	The CBI observed gaps in CASP STOR frameworks, surveillance tooling, and ability to identify/manipulate on-chain behaviours. 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.	Early supervisory assessments found governance, control frameworks, and risk management to be uneven. Some firms require significant uplift to meet minimum expectations.

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

The Central Bank of Ireland’s 2026 Regulatory & Supervisory Outlook marks the first full supervisory cycle with **MiCAR regulated Crypto Asset Service Providers (CASPs)** entering the Irish regulatory perimeter. What companies should focus on next are:

CASPs are expected to mature rapidly into “institution grade” firms

Many crypto businesses are operating under regulatory oversight for the first time. Early supervisory assessments have already highlighted uneven governance, weak control frameworks, and Boards lacking financial services risk experience. CASPs must now uplift their governance and internal controls to match standards applied to banks, payments firms, and MiFID.

MiCAR whitepaper volumes mean deeper supervisory scrutiny

In 2025, the CBI received over 300 MiCAR Title II whitepapers, far exceeding expectations and demonstrating the pace of innovation in the sector. This has triggered a heightened focus on risk disclosure accuracy, suitability information, conflicts of interest, and token economic transparency in 2026.

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

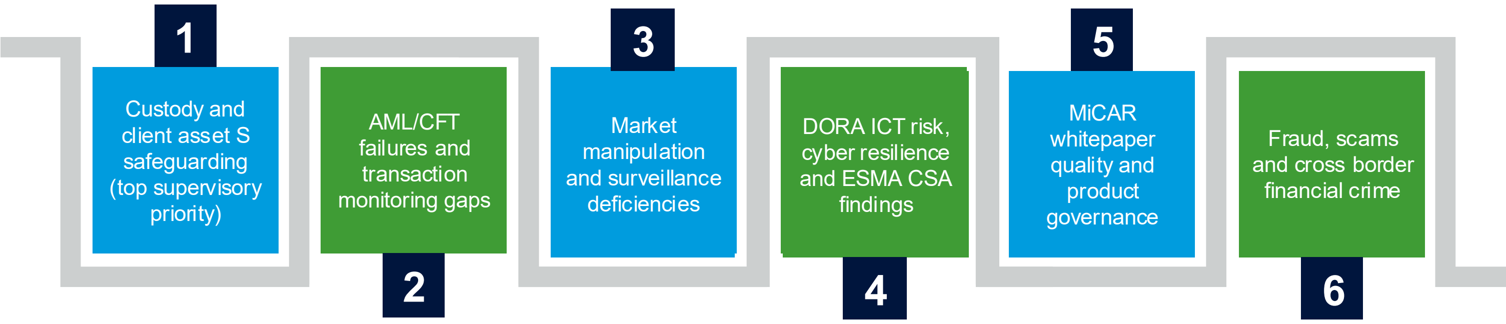
Because crypto environments are pseudonymous, borderless, and technology dependent, the CBI considers CASPs to be high risk for AML/CFT breaches, fraud, misconduct, cyberattacks, and market manipulation. Supervisors will use enhanced data collection, targeted inspections, and an ESMA led cyber–Common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

Immediate actions for crypto companies to take in 2026 (Q2–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 ▪ Deploy blockchain analytics tools to detect cross chain flows, mixers/tumblers, sanctions exposure, and pseudonymous layering activity. ▪ Strengthen onboarding, KYC and EDD procedures.
Deliver DORA operational resilience compliance	▪ Map Critical or Important Business Services (CIBS) for crypto activities (hot/cold wallets, trading engines, blockchain nodes, APIs, custody integrations). ▪ 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. ▪ Strengthen suitability frameworks for complex, leveraged, or illiquid crypto offerings.
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. ▪ Implement SEAR/IAF responsibility mapping for crypto leadership roles (Head of Custody, CTO, MLRO). ▪ Provide Board training on MiCAR, DORA, cyber risks, and crypto-market integrity obligations.

Areas of expected supervisory intensification in 2026



Area	Rational 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. The CBI will intensify inspections of: • private key storage and multisig controls • wallet segmentation and cold storage • third party custody reliance
2. AML/CFT failures and transaction monitoring gaps	Supervision will target: • effectiveness of blockchain analytics usage • sanctions screening • typology detection in pseudonymous environments • quality of enhanced AML REQs
3. Market manipulation and surveillance deficiencies	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
4. DORA ICT risk, cyber resilience and ESMA CSA findings	CASPs should anticipate intrusive testing of: • cyber incident response • API & trading engine resilience • cloud dependency and exit strategies • CIBS mapping quality
5. MiCAR whitepaper quality and product governance	Scrutiny will increase around: • risk disclosures • token economics transparency • conflicts of interest • marketing alignment with regulatory obligations
6. Governance, board oversight and culture	Supervisors will examine whether Boards: • understand crypto specific risks • challenge management effectively • maintain clear accountability under SEAR/IAF • Governance maturity is highly variable across CASPs

How we can help

Custody and client asset safeguarding

Our client-selectable services include:

- Independent review of private key management, multisig 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.

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.

Operational resilience and DORA compliance

Our client-selectable services include:

- DORA aligned ICT, cyber, incident management and recovery assessments.
- Mapping of crypto specific Critical or Important Business Services (CIBS) (e.g., wallets, trading engines, blockchain nodes, custody integrations).
- Testing of cloud, protocol and API dependencies.
- Support for European Securities and Markets Authority (ESMA) led cyber-common Supervisory Action (CSA) expectations.

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.

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.

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

catherine.brittain@rsmuk.com

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