Plenitude
Inspiring confidence, delivering excellence

From Fines to Fixes

What Crypto Firms Can Learn from Recent Enforcement Actions

May 2025

Plenitude Insights

Executive Summary

As regulatory scrutiny of the crypto industry intensifies, enforcement actions send a clear message: crypto compliance must meet the standards already expected from their traditional finance (TradFi) peers.

This paper explores recent regulatory actions against Crypto Asset Service Providers (CASPs) and traditional financial institutions to uncover common compliance failures across key control areas such as customer due diligence, sanctions, governance, and transaction monitoring.

Firms that treat compliance as a strategic enabler—rather than a regulatory burden—will be better positioned to thrive in an increasingly regulated crypto ecosystem.

Key takeaways:

- Regulators are raising the bar for CASPs, applying expectations that are similar to those from TradFi peers.
- Recent fines and enforcement actions reveal recurring failings, particularly in governance, customer due diligence and transaction monitoring.
- Proactive compliance is essential: CASPs must shift from a reactive mindset to building mature, scalable, and auditable frameworks.
- Using enforcement insights as a roadmap, CASPs can reduce regulatory risk, build trust, and enable sustainable growth.

The Evolving Regulatory Landscape for CASPs

Crypto Asset Service Providers (CASPs) no longer operate on the fringes of financial regulation. As the industry becomes more integrated into the mainstream financial system, regulators are increasingly applying the same expectations and scrutiny used for traditional financial institutions (FIs).

In jurisdictions such as the USA, UK and EU, CASPs already face obligations comparable to those of traditional financial institutions in areas such as anti-money laundering, counter-terrorist financing, and sanctions compliance. Recent developments, including the introduction of the EU's Markets in Crypto-Assets Regulation (MiCA), are reinforcing this shift by extending requirements across governance, disclosures, and market conduct.

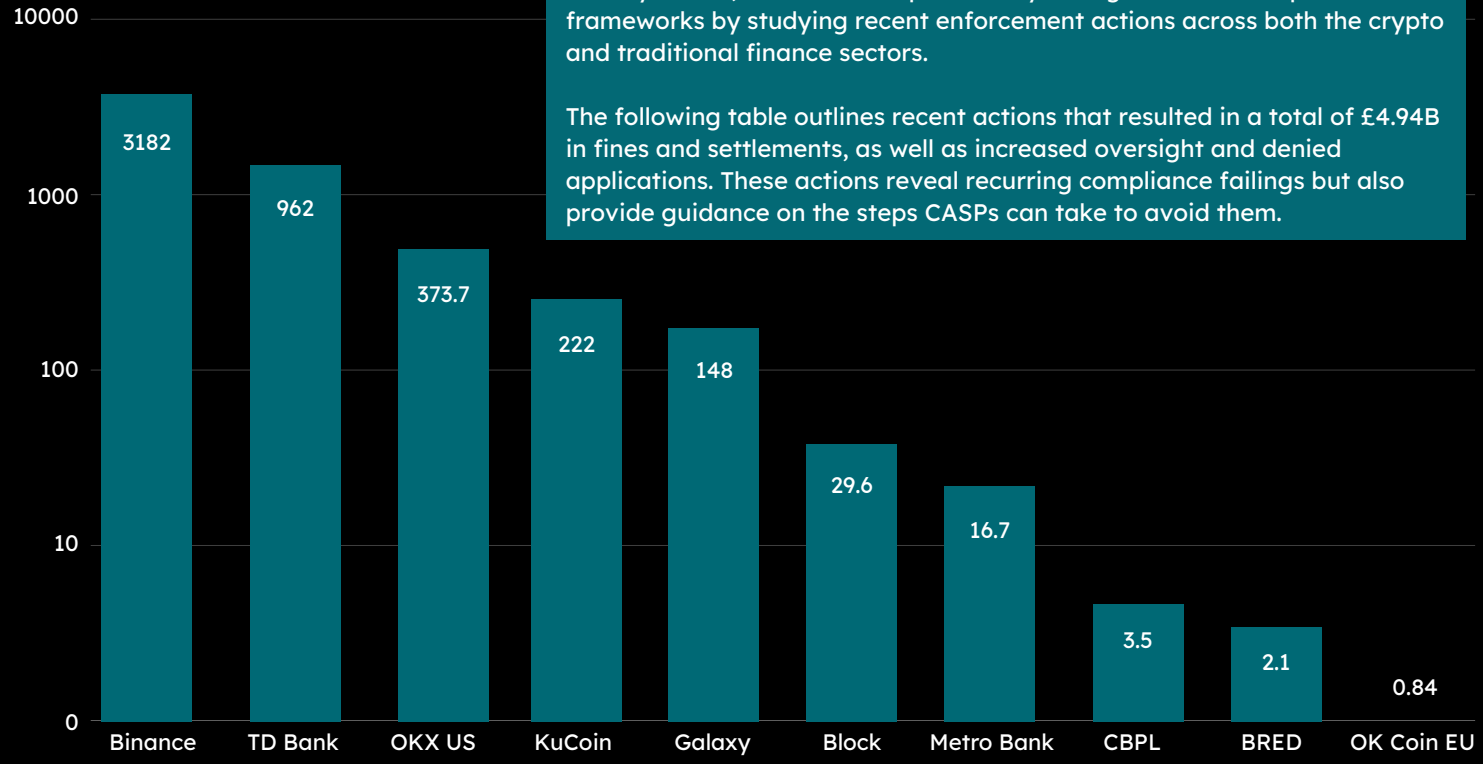
While this alignment can appear burdensome at first sight, CASPs are not navigating uncharted territory. Instead, they can draw on several years of regulatory guidance, enforcement outcomes, and established best practices to build resilient compliance frameworks from the outset.

This shift carries two key implications:

- First, CASPs can learn from the regulatory path already taken by the financial sector, using it as a practical roadmap for what good looks like.
- Second, as the scope of compliance obligations broadens, meeting minimum requirements is no longer sufficient. CASPs must adopt a proactive, end-to-end approach to compliance to keep pace with regulatory change and avoid future enforcement.

To stay ahead, CASPs should proactively strengthen their compliance frameworks by studying recent enforcement actions across both the crypto and traditional finance sectors.

The following table outlines recent actions that resulted in a total of £4.94B in fines and settlements, as well as increased oversight and denied applications. These actions reveal recurring compliance failings but also provide guidance on the steps CASPs can take to avoid them.



Fines by Firm: Who Paid the Most? (£ Million)

Log scale

Company	Date	Country / Regulator	Description	Regulatory Action
Block	Apr 2025	USA – NYDFS	Deficiencies in AML programme, including inadequate customer identification procedures and transaction monitoring.	£29.6 million settlement
Galaxy Digital	Apr 2025	USA – OAG	Allegations of market manipulation related to LUNA.	£148 million settlement
OKCoin - EU	Apr 2025	Malta – FIAU	Deficiencies in AML and CFT compliance framework.	£0.84 million fine
Zeux	Mar 2025	UK – FCA	Concerns over the design of AML controls, including inadequate risk assessments, insufficient customer due diligence and deficient processes for reporting suspicious activity.	Rejected application for registration as a cryptoasset exchange
OKX - US	Feb 2025	USA – Attorney's Office (SDNY)	AML violations and unlicensed activities in the US.	£373.7 million fine
KuCoin	Jan 2025	USA – Attorney's Office (SDNY)	Operation of an unlicensed money transmitting business and failure to implement effective AML and KYC programs.	£222 million fine

Company	Date	Country / Regulator	Description	Regulatory Action
Metro Bank	Nov 2024	UK - FCA	Deficiencies in the systems and controls to adequately monitor transactions	£16.7 million fine
TD Bank	Oct 2024	USA - FinCEN	AML compliance failures, including inadequate transaction monitoring that allowed illicit activities to go undetected.	£962 million penalty & 4-years independent monitorship
CBPL	Jul 2024	UK – FCA	Failing to abide by the Voluntary Requirement (VREQ) that forbade it to provide services to high-risk customers.	£3.5 million fine
BRED	Jun 2024	France – ACPR	Deficiencies in AML/CFT framework.	£2.1 million fine and public reprimand
Binance	Nov 2023	USA – CFTC, FinCEN, OFAC	Violations of the Bank Secrecy Act (BSA) and sanctions, as well as unlicensed money transmitting.	£3,182 million settlement
Bykep	Sep 2022	France – AMF	Severe AML/CTF compliance failures, including unauthorized transactions on clients' wallets and inadequate KYC procedures.	Withdrawal of digital asset service provider registration

Common Failing Areas - Lessons from Regulatory Actions

Based on our analysis of a sample of 12 cases, recent regulatory actions against CASPs, payment service providers, and traditional FIs have revealed recurring compliance deficiencies across several key control areas, indicating clear themes of lessons learned.

Key Lessons

1 Embed Ongoing Oversight and Testing

- Implement structured MI dashboards, escalation protocols, and issue management frameworks.
- Conduct regular, independent testing of controls, ensuring they are risk-based, current, and effective against evolving threats.

2 Strengthen Governance and Resourcing

- Clearly document policies, procedures, and team responsibilities.
- Empower compliance personnel with the authority, experience, and resources needed to enforce controls.
- Scale compliance with business growth to prevent backlogs and control failures.

3 Build Robust Transaction Monitoring and Reporting Systems

- Calibrate TM rules for on- and off-chain activity based on customer and product risk profiles, rather than using generic settings.
- Perform periodic data completeness checks, and QA/QC controls to ensure thorough monitoring and timely SAR filings.

4 Establish Risk-Based and Holistic Assessments

- Conduct comprehensive and well-documented BWRAs and CRAs that incorporate all relevant risk factors, jurisdictions, and customer behaviours.
- Ensure every customer is risk-rated at onboarding and reviewed periodically, especially in response to profile or policy changes.

5 Enhance CDD and Monitoring

- Mandate complete KYC before product access and block attempts to bypass controls.
- Integrate geolocation, IP data, and wallet ownership verification (e.g., AOPP, Satoshi Test) into CDD and EDD processes.

Control Area: Governance

Finding 1: Failure to properly document procedures and operational processes, including roles and responsibilities of key staff

- **CBPL:** Did not develop documented processes and procedures to comply with VREQ requirements forbidding it from onboarding high-risk customers, nor did it document roles and responsibilities of teams involved in these processes.
- **TD Bank:** The designated BSA Officer lacked the authority, independence, control, and accountability necessary to administer an effective AML compliance program.
- **Metro Bank**: Lacked clear ownership for the ongoing monitoring of the automated transaction monitoring system, including ensuring data completeness.

Lessons Learned

- Clearly document policies, procedures and controls, including the roles, and responsibilities of teams involved in their execution and oversight.
- Ensure that key personnel are empowered with sufficient authority and resources to enforce compliance effectively.

Finding 2: Failure to allocate sufficient resources to the Compliance programme along with the growth in the business

- **Block**: The AML program did not keep pace with the growth of the company, notably resulting in significant backlogs of transaction monitoring alerts and unacceptable delays in filing Suspicious Activity Reports (SAR).
- **TD Bank**: AML staffing was not proportionate to the bank's size, risk profile and ongoing compliance concerns, with the bank insisting on a flat cost paradigm in the face of mounting backlogs and compliance issues.

Control Area: Governance

Lessons Learned

- Compliance resources must scale in line with business growth.
- Use appropriate MI and activity indicators to anticipate operational bottlenecks such as alert backlogs or delays in filing SARs.

Finding 3: Inefficient escalation processes or failure to act on escalated issues

- **Metro Bank:** Risks and issues that were known at relatively junior levels were either not escalated in a timely manner or, when escalated to committees or senior management, were not acted upon.
- **TD Bank:** Failed to escalate significant issues to senior management or the Board in a timely manner.
- **BRED**: Failure to act on issues identified by Internal Audit.

Lessons Learned

- Establish clear escalation protocols and adopt an issue management framework to ensure timely resolution and accountability at senior levels.
- Ensure appropriate documentation of escalations and action taken to address issues and prevent recurrence.

Control Area: Governance

Finding 4: Insufficient or inadequate MI

- **Metro Bank:** Lacked MI to detect TM system data feed errors, delaying senior management awareness.
- **CBPL:** Did not implement MI to track VREQ-related data, failing to identify breaches in control design.

Lessons Learned

- Develop comprehensive MI dashboards and apply trend analysis to identify anomalies and issues, including resource constraints.

Finding 5: Failure to appoint staff with sufficient experience or to provide appropriate training

- **TD Bank:** Appointed AML managers without any previous AML experience and failed to ensure that employees received appropriate training
- **OKCOIN (EU):** Training was not tailored to the company's own AML policies and procedures

Lessons Learned

- Appoint qualified personnel and provide training tailored to internal policies and regulatory expectations.

Control Area: BWRA

Finding 1: Incomplete or incorrect risk factors considered

- **Zeux:** Did not consider all risk factors required by applicable regulation and thus failed to assess inherent business risks comprehensively. Besides, the risks presented (e.g. controls or control failings) evidenced a misunderstanding of the purpose of the BWRA.
- **OKCOIN (EU):** Failed to adequately assess the risks of specific categories of products and services and of potential risk exposures arising from other jurisdictions.

Lessons Learned

- BWRA must comprehensively consider all required risk factors and accurately reflect the business's inherent risks, rather than merely listing control failures.

Finding 2: Unclear or insufficiently detailed BWRA Methodology

- **Zeux:** The methodology lacked sufficient detail to articulate how inherent risk, control effectiveness and residual risk were assessed and derived.
- **OKCOIN (EU):** Failed to demonstrate that it had considered the statistical data at its disposal to form a clear and substantiated opinion on the threats and vulnerabilities to which the business was exposed.

Lessons Learned

- Clearly document the BWRA methodology for assessing inherent risk, control effectiveness, and residual risk, supported by appropriate data and rationales.

Control Area: Customer Risk Assessment

Finding 1: Inadequate CRA methodology

- **OKCOIN (EU):** Adverse media screening results were not incorporated into the CRA. Besides, although products (coins) were classified as “high-risk” and “low-risk,” there was no clearly defined methodology to support such classification. Insufficient consideration of customers’ source of funds.
- **Zeux:** Lacked a CRA tool and there was no evidence of a customer risk rating methodology. A single risk factor dominated the entire customer risk rating, ignoring the broader customer profile.

Lessons Learned

- Document a CRA methodology that assesses risk in a holistic manner considering all applicable risk factors and ensure that its application results in reliable customer risk ratings.

Finding 2: Failure to Risk-Rate All Customers

- **TD Bank:** Some customers were not risk-rated or were incorrectly risk-rated, and issues identified were not addressed for a prolonged period.
- **OKCOIN (EU):** Failed to carry out a CRA upon establishing a business relationship for about half of sampled customers

Lessons Learned

- Every customer must be risk-rated during onboarding and that the ratings are reviewed periodically. Systems should flag customers with missing or outdated risk ratings.

Control Area: Customer Due Diligence

Finding 1: Failure to apply KYC measures

- **Binance and KuCoin:** Allowed users to access products without completing KYC.
- **TD Bank:** Failed to sufficiently collect and review customer information to develop customer risk profiles and identify high-risk accounts.
- **BRED & OKCOIN (EU):** Failed to collect information such as customers' anticipated level of activity and occupation during the onboarding process.
- **Block:** Failed to prevent customers from setting up multiple accounts to bypass the transaction limits and triggers. Likewise, exited customers could be re-onboarded by using restricted accounts for which KYC was not required.
- **OKX (US):** Allowed customers to access products and services without completing KYC, and allowed 3rd party "non-disclosure brokers" to place trades for customers without providing information to OKX about the customers on whose behalf orders were placed.

Lessons Learned

- Enforce mandatory completion of KYC prior to product access and implement controls to prevent circumvention via duplicate or third-party accounts.
- Collect, verify, and document sufficient customer information during onboarding to establish a comprehensive risk profile.

Control Area: Customer Due Diligence

Finding 2: Inadequate geofencing measures

- **OKX (US):** Failed to prevent business relationships with customers in the US and, in some cases, actively advised potential customers on how to conceal their US presence and circumvent controls.
- **KuCoin:** Collected data like IP address and login history but failed to leverage these for geofencing.
- **Binance:** Took active steps to maintain US customers through use of offshore entities and provision of false information, and by ignoring mismatches between log-in IP addresses and KYC information to prevent access by customers from blocked countries.

Lessons Learned

- Utilise other customer information, such as IP address and location data, to proactively detect and block access from restricted jurisdictions.

Control Area: Enhanced Due Diligence

Finding 1: Inadequate EDD measures

- **Zeux:** EDD measures and triggers were not aligned with the regulatory requirements.
- **Bykep:** Failed to implement EDD measures for high-risk customers
- **TD Bank:** Failed to apply enhanced monitoring for high-risk customers.
- **OKCOIN (EU):** Failed to implement EDD measures for a significant proportion of high-risk customers and failed to collect evidence of ownership or control over private wallets for several high-risk customers, despite these presenting significant transaction volumes.

Lessons Learned

- Ensure that EDD triggers and the resulting measures are aligned with regulatory requirements.
- Verify ownership of high-risk self-hosted wallets using appropriate methods (e.g., AOPP, Satoshi Test, or Manual Signing).

Control Area: Ongoing Due Diligence

Finding 1: Failure to complete event-driven reviews

- **Binance and KuCoin:** Significant changes in compliance program (i.e. introducing mandatory KYC process) did not trigger a review of existing customers.
- **Block:** Failed to identify changes to customer initial KYC information to trigger an event-driven Review.
- **CBPL:** Failed to ensure that changes in customer information were aligned with VREQ requirements.

Lessons Learned

- Treat significant customer profile changes as triggers for event-driven reviews to ensure updated customer risk assessments.
- Accompany changes in KYC procedures or components of the CRA methodology (e.g. country / industry risk lists) with a review of the KYC files of impacted existing customers.

Finding 2: Failure to conduct Periodic Reviews on time

- **OKCOIN (EU):** Failed to conduct periodic reviews in accordance with the pre-defined review frequency.
- **TD Bank:** Periodic reviews for high-risk customers were conducted too infrequently, failing to follow a risk-based approach.

Lessons Learned

- Systems should be in place to flag the scheduled periodic review to ensure pre-defined periodic review frequencies are followed.
- High risk customers should be subject to periodic review at least annually.

Control Area: Ongoing Due Diligence

Finding 3: Inadequate ODD measures

- **TD Bank:** Failed to review transaction behaviour as part of periodic reviews (e.g. discrepancies between expected and actual activity, and red flags in customer activity).
- **OKCOIN (EU):** Failed to take necessary steps to obtain up-to-date and valid documentation after existing documents had expired.

Lessons Learned

- Periodic reviews must evaluate actual customer transaction behaviour in addition to confirming the continued validity of documentation already provided.

Control Area: Transaction Montoring

Finding 1: Inadequate set-up of rulesets in automated transaction monitoring systems

- **BRED:** Certain customers were either partially or fully excluded from transaction monitoring, which led to a reduced number of alerts.
- **TD Bank:** Used “off-the-shelf” scenarios that were not tailored to its business and products and consequently failed to assess if scenarios adequately mitigated risks specific to their products. Besides, it did not differentiate transaction monitoring rules based on customer risk levels.
- **BRED:** The configuration of automated detection scenarios was incorrect, with thresholds sometimes too broad or too high relative to the characteristics of customer transactions, resulting in an ineffective transaction monitoring system. The bank also did not adequately segment its customers, preventing the application of proportionate transaction monitoring rules.
- **Block:** Incorrectly applied risk-based approach to act on terrorism-connected wallets and inadequate risk rating of transactions with exposure to mixers (rated as Medium risk despite regulatory guidance to the contrary).

Lessons Learned

- Calibrate TM rules to reflect the firm’s products, customer risk profiles, and typologies, rather than relying on “out-of-the-box” standard settings.

Control Area: Transaction Montoring

Finding 2: Lack of blockchain analytics tools

- **Bykep:** No use of surveillance tools adapted for cryptoassets despite representations made during the registration process

Lessons Learned

- Implement blockchain analytics tools to effectively screen wallets and monitor on-chain transactions.

Finding 3: Inadequate scope of transaction monitoring

- **BRED:** Certain customers were either partially or fully excluded from transaction monitoring, which led to a reduced number of alerts.
- **Metro Bank:** Errors in the data feed resulted in transactions not being subject to automated monitoring, and there was no mechanism in place to ensure that all relevant transactions were fed into the monitoring system.

Lessons Learned

- Implement blockchain analytics tools to effectively screen wallets and monitor on-chain transactions.

Control Area: Transaction Montoring

Finding 4: Incorrect or insufficient review of transaction monitoring alerts

- **OKCOIN (EU) & BRED:** TM alerts were not properly reviewed or investigated and were sometimes discounted without sufficient justification.

Lessons Learned

- Implement QA/QC controls to ensure alerts are properly reviewed and escalated where needed, as well as ensuring that comments to close alerts allow for appropriate explainability of action taken.

Control Area: SARs

Finding 1: Non-Reporting or delayed reporting of Suspicious Activities

- **Binance, KuCoin, and OKCOIN (EU):** Did not file SARs despite processing suspicious and potentially criminal transactions.
- **TD Bank:** Underinvested in compliance resources, resulting in significant backlogs for investigating potential suspicious activities.
- **Block:** Delay in reporting suspicious activities due to significant backlog of transaction monitoring alerts.

Lessons Learned

- Maintain adequate compliance resources to manage alert volumes and file SARs in a timely manner. Use MI to anticipate backlogs.

Finding 2: Deficient procedures for SAR Reporting

- **Zeux:** Lacked documented procedures for internal and external SAR reporting and failed to document information regarding how to request a DAML and the importance of doing so.
- **TD Bank:** Failure to apply restrictions or risk mitigation measures for customers subject to SAR filings.

Lessons Learned

- Develop and maintain appropriate SAR procedures, covering both internal and external filing, guidance related to defence/consent requests (if applicable) and post-SAR customer risk mitigation measures.

Control Area: Sanctions

Finding 1: Lack of a sanction compliance framework

- **Bykep:** Failed to establish a framework to comply with asset freezing measures.

Lessons Learned

- Establish and document a comprehensive sanctions compliance programme aligned with regulatory expectations.

Finding 2: Inadequate sanctions screening

- **Bittrex:** Screened transactions only against SDN and other lists, but not for customers or transactions with links to sanctioned jurisdictions.
- **Block:** Service providers and employees were not subject to ongoing screening against OFAC sanction lists.

Lessons Learned

- Screen customers, transactions, service providers, and employees both at onboarding and on an ongoing basis, and against all applicable lists.

Control Area: Sanctions

Finding 3: Failure to offboard customers from sanctioned countries

- **Binance and CoinList:** Failed to offboard customers from sanctioned countries despite having evidence such as IP location and KYC data.

Lessons Learned

- Leverage all available information to identify and offboard clients outside the firm's risk appetite.

Control Area: Market Conduct

Finding 1: Failed to disclose Conflict of Interest

- **Galaxy Digital:** Failed to disclose it was selling substantial portions of LUNA into the public markets while making public statements promoting LUNA.

Lessons Learned

- Identify and disclose conflicts when issuing promotional materials or public statements.

Finding 2: Provision of misleading and inaccurate information

- **Galaxy Digital:** Presented false and misleading statements and information on social media, podcasts, and news to inflate the token price, and disclosed price-sensitive information without conducting proper due diligence to ensure its accuracy.

Lessons Learned

- Perform due diligence before making public statements involving price-sensitive information.

Control Area: Control Testing, Monitoring and Assurance

Finding 1: Inadequate calibration or ongoing review of Compliance Tools

- **CBPL:** Failed to calibrate the CDD tools to fulfil the VREQ requirements and failed to conduct ongoing monitoring and testing of the effectiveness of the controls in place to ensure compliance with the VREQ.
- **Metro Bank and TD Bank:** Did not conduct proper testing or gap assessments of transaction monitoring systems.

Lessons Learned

- Conduct periodic calibration and testing of compliance systems (e.g., CDD, TM), ensuring the tools are fit for purpose, aligned with regulatory requirements and performing as expected.

Finding 2: Insufficient or inadequate independent testing

- **TD Bank:** Insufficient independent testing that failed to identify material gaps, resulting from a combination of its limited scope, inappropriate methodologies that overlooked key risks and control factors and inappropriate prioritisation based on underlying risks

Lessons Learned

- Maintain an independent compliance testing programme and methodology.
- Ensure testing is risk-based and methodologically sound to uncover material deficiencies.

Strengthening Compliance Frameworks: Practical Actions for CASPs

Recent enforcement actions have reinforced that CASPs are being held to the same standards as traditional financial institutions. As regulatory expectations increase and scrutiny deepens, particularly for firms operating across borders, it is essential to take a proactive and structured approach to compliance.

Firms should focus on the following actions to strengthen their frameworks and reduce enforcement risk:

1. Use available regulatory resources

There is no need to start from scratch. CASPs should leverage different existing resources, including:

- Regulations relevant to their jurisdiction and business model
- Guidance from national regulators and international bodies such as the FATF
- National Risk Assessments to understand jurisdiction-specific threats and priorities
- Recent enforcement actions and regulatory findings to benchmark against market expectations
- Communications from regulators, such as Dear CEO letters, newsletters, and thematic reviews that often signal current areas of focus

2. Conduct regular, independent assessments

It is essential for CASPs to conduct regular, proactive independent assessments of their compliance control frameworks. These reviews help ensure that these frameworks remain aligned with current regulatory standards and best practices and are operating effectively in practice. Where gaps or deficiencies are identified, they should be promptly escalated and remediated with appropriate action that mitigates the risk of recurrence.

3. Engage external expertise where appropriate

Independent external assessments can help identify blind spots, provide benchmarking, and support remediation planning. At Plenitude, we work closely with firms to assess, strengthen, and future-proof their compliance and financial crime frameworks across the full lifecycle, from gap assessments and policy development to delivering transformation programmes and strengthening governance. As an appointed member of the FCA's Skilled Person Panel for Financial Crime, we bring deep expertise in reviewing control frameworks and in providing actionable, practical and proportionate guidance aligned to regulatory expectations.

4. Recognise compliance as a strategic asset

Strong compliance frameworks are not only a regulatory requirement but also a business enabler. They reduce operational and reputational risk, build trust with stakeholders, and support safe, scalable growth in an increasingly regulated market.

Conclusion

The evolution of crypto regulation presents an opportunity to build stronger and more resilient businesses. Compliance is not a checkbox exercise—it's the foundation for long-term stability, growth, and trust. By acting early, drawing on lessons from other sectors, and using existing guidance as a starting point, firms can position themselves to meet regulatory expectations and contribute to a more sustainable and credible industry.

About Plenitude

Plenitude provides market-leading Financial Crime Compliance (FCC) advisory, transformation, technology, data analytics, and managed services. We are committed to building a secure financial system, safeguarding society, and empowering our clients to meet their regulatory obligations.

Plenitude's Digital Assets Practice has assembled a team that brings deep knowledge of cryptoassets, which is essential to understanding crypto business models and the associated risks. We can also help traditional finance firms develop their knowledge of this industry, make informed decisions about their crypto strategy and thus seize the emerging opportunities of the emerging digital economy.

About the authors:

Gary Yeung is a Senior Consultant at Plenitude Consulting in the Digital Assets Practice with over 5 years of industry experience. He comes from a crypto-native background working in one of the largest digital asset trading platforms, specialised in corporate strategy, market research and compliance within the digital asset industry. He has an in-depth knowledge of digital asset-related concepts and regulatory frameworks in the key market regions such as the UK, EU, Hong Kong, Singapore and the US. Gary is a CFA Charter holder and holds MSc in Finance and Financial Technology (FinTech) at Henley Business School, University of Reading.

Manuel Fajardo, Director and Head of our Digital Assets Practice, brings over 17 years of global asset management experience, focusing on compliance, internal control, and audit functions across Paris, London, and Los Angeles. With over eight years in the cryptoassets industry, Manuel advises crypto firms on compliance, educates traditional finance companies on crypto's significance and the evolving regulatory landscape, and actively contributes to regulatory discussions through industry bodies. Before joining Plenitude, he established compliance frameworks for a major investment management group, emphasising AML, International Sanctions, and Financial Promotions/Distribution.

To learn more, email us at enquiries@plenitudeconsulting.com