DFSB

DIGITAL FIDUCIARY STANDARDS BOARD

Handbook on Digital Fiduciary Investment Standards

1st Edition | December 2025

TABLE OF CONTENTS

Disclaimer iii

Preface iv

Standard 1: Fiduciary Governance 1

Standard 2: Regulatory Compliance 15

Standard 3: Conflicts of Interest 32

Standard 4: Investment Policy & Governance 46

Standard 5: Investment Operations 65

Standard 6: Risk Management 94

Standard 7: Leverage & Liquidity Management 109

Standard 8: Safekeeping of Assets 129

Standard 9: Counterparty Management 154

Standard 10: Valuation and Performance 167

Standard 11: Treasury Controls 190

Standard 12: Technology & Cybersecurity 209

Standard 13: Client Due Diligence 226

Standard 14: Transparency & Communication 239

Standard 15: Organizational Continuity 254

Standard 16: Responsible Investment Stewardship 268

Standard 17: Service Providers & Professional Relationships 278

Appendix: Glossary of Terms 295

Endnotes 307

DISCLAIMER

This Handbook on Digital Fiduciary Investment Standards offers guidance from the Digital Fiduciary Standards Board (DFSB) for investment managers in digital asset markets. It emphasizes that these standards are recommendations, not legal requirements, and do not guarantee regulatory compliance or operational success. Firms are responsible for adhering to applicable laws and should seek professional advice for their specific circumstances.

Regulatory developments in digital assets are rapid and ongoing. Standards reflect the landscape at publication but may become outdated as new regulations and guidance emerge. Firms must stay informed and adapt accordingly.

DFSB disclaims warranties regarding the standards' accuracy or suitability. Implementation does not ensure access to capital, regulatory approval, or operational success, as investment involves inherent risks. The organization and its affiliates are not liable for damages resulting from reliance on these standards.

Standards should be tailored to each firm's unique context, strategies, and client needs. Mechanical application without considering specific circumstances may be inappropriate. Firms must exercise independent judgment and conduct due diligence on service providers and operational choices.

Use of these standards does not imply certification or endorsement by DFSB. Standards will evolve with market and regulatory changes, and firms should monitor updates. Each firm remains responsible for its compliance, risk management, and fiduciary duties, supplementing but not replacing internal policies developed with professional guidance.

While primarily reflecting U.S. regulations, firms in other jurisdictions must also comply with local laws. By using this handbook, users agree to its disclaimer; non-agreement means they should not rely on these standards.

© 2026 Digital Fiduciary Standards Board (DFSB). All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means without prior written permission.

PREFACE

The Digital Fiduciary Standards Board (DFSB), an independent nonprofit, has created this handbook to bridge the gap between institutional allocators and digital asset managers. The industry is at a pivotal point, with institutional investors recognizing digital assets as a legitimate asset class. However, many disqualify crypto-native managers not due to strategy issues but because they cannot demonstrate fiduciary-grade management of client capital. Conversely, traditional asset managers have established fiduciary frameworks but lack the specific knowledge needed for digital asset custody, smart contract risks, and blockchain operations.

The challenge is primarily fiduciary in nature. Crypto-native managers understand the markets and technology but struggle to prove they meet legal duties such as care, loyalty, and prudence required by institutional investors. The handbook aims to address this by translating proven fiduciary standards into digital asset-specific guidelines that are practical and applicable.

Standards Development

These standards were developed through rigorous analysis of fiduciary requirements, regulatory expectations, and digital asset operational realities. Development incorporated:

- Consultation with institutional allocators to identify fiduciary requirements and disqualifiers in manager evaluation
- Expertise from managers with experience in building institutional-grade digital asset platforms
- Review of SEC, FINRA, CFTC, and international regulations relevant to digital assets
- Input from service providers such as administrators, auditors, custodians, and legal counsel

Each standard addresses real questions allocators ask during due diligence about whether managers can fulfill fiduciary obligations. Standards specify implementable frameworks that demonstrably satisfy fiduciary requirements while remaining practical for emerging managers.

Scope and Application

We wrote this handbook to serve investment managers, allocators and institutional investors across jurisdictions while recognizing that specific regulatory requirements vary by region. Where regulatory mandates apply in certain jurisdictions, relevant considerations are identified. However, these are standards and guidance, not legal requirements. Recommendations do not replace applicable legal or regulatory obligations, which are likely more detailed than the practices described.

Firms remain solely responsible for ensuring compliance with all applicable laws, regulations, and contractual obligations. Professional legal, compliance, accounting, or other advice should be obtained where appropriate—these standards are not a substitute for such counsel.

Intended Audiences

The handbook serves three primary audiences, each playing essential roles in bridging institutional capital and digital asset management:

- *Digital asset investment managers seeking institutional capital:* If you manage, or intend to manage, capital for institutional allocators, these standards define fiduciary expectations for consideration. Firms managing exclusively retail capital may find standards overly prescriptive.
- *Institutional allocators evaluating digital asset managers:* These standards provide due diligence frameworks, identify critical fiduciary areas, and establish baseline expectations for fiduciary-grade management.
- *Service providers supporting digital asset managers:* Auditors, administrators, custodians, and legal counsel require understanding of fiduciary expectations to deliver appropriate services.

Structure and Navigation

The handbook contains 17 standards covering every fiduciary area that institutional allocators assess during due diligence. Each standard follows a consistent structure providing operational frameworks, practitioner insights, allocator due diligence considerations, common pitfalls and remediation, and key controls and documentation requirements. Standards are intentionally detailed—institutional allocators reject vague descriptions and require specific frameworks with documented procedures.

Implementation Philosophy

These standards provide a flexible, outcome-based framework for fiduciary practices, scaled to firm size and complexity. They avoid prescribing specific vendors or technologies, allowing firms to tailor their approaches while addressing digital asset realities. Implementation is iterative; firms can seek institutional capital without full compliance, as allocators evaluate fiduciary progress through controls and sophistication. Use these standards to demonstrate fiduciary capability, protect client assets, and meet legal duties required by institutional investors.

Acknowledgments

The DFSB thanks all stakeholders—allocators, managers, service providers, and the digital asset community—for their valuable contributions in developing practical standards that promote innovation and fiduciary responsibility. Standards will continue to evolve as markets develop, regulations change, and best practices emerge. We welcome feedback from practitioners, allocators, and service providers.

DFSB may update this Handbook periodically to reflect regulatory developments, market evolution, and emerging operational best practices. Managers should confirm they are using the current version available at dfsb.org. Version number and publication date appear on the cover page.

The Digital Fiduciary Standards Board (DFSB)
201 Clearwater Drive | Suite 1703
West Palm Beah, FL 33401
info@dfsb.org

STANDARD 1: FIDUCIARY GOVERNANCE

Firms must establish and maintain effective governance structures. This includes board oversight with appropriate expertise and authority over operations, risk-taking, and strategic direction; a clear organizational structure with defined roles, responsibilities, and reporting lines; and comprehensive policies and procedures covering all operational areas. Firms must implement succession planning and knowledge management for critical positions to mitigate key person risk and conduct regular assessments and monitoring of governance effectiveness with documented review processes.

Fiduciary governance defines who has the authority to make decisions, how accountability flows within the organization, and whether oversight functions independently. It determines if there is a single point of failure in investment strategy, operational execution, or asset control—key risks that institutional allocators consider before investing capital.

Standard 1 requires firms to demonstrate that no single person controls investment decisions, operational processes, or asset custody without oversight. This standard addresses three core governance issues that institutional allocators won't accept: boards lacking independence or digital asset expertise, management structures that concentrate power without checks, and policies that are written but ineffective in practice.

Maintaining this standard involves establishing independent board oversight with digital asset expertise, developing professional management with distinct roles, enforcing policies with documented compliance, planning succession for key roles, and forming committees that challenge rather than merely approve management decisions. Firms that do not meet these requirements face significant risks from key personnel and operational vulnerabilities, disqualifying them from attracting institutional capital.

1.1 BOARD COMPOSITION AND STRUCTURE

A board of directors oversees management, offers strategic advice, and has fiduciary responsibilities. In digital assets, boards need to know basic investment rules and also

understand risks like smart contract flaws, how assets are stored, and protocol issues. The makeup of the board shows whether it truly supervises or just meets legal requirements.

1.1.1 BOARD SIZE AND INDEPENDENCE

Your board should have at least three directors. If the assets under management go over $100 million, increase the number of directors to five or seven. At least one, preferably two, directors should be truly independent. This means they should not have any important relationships, family ties, or financial dependence on the company. Independence means the director can question management freely without worrying about losing pay or important relationships. Directors who get consulting fees, work as outside lawyers, or have family members working for the company are not considered independent.

Essential board expertise includes:

- Traditional asset management experience establishes credibility with institutional allocators and provides context for adapting proven controls to digital assets
- Digital asset operational proficiency enables meaningful oversight of blockchain-specific risks, custody architectures, and protocol evaluation
- Enterprise risk management capability provides frameworks for complex threat assessment, control design, and incident response
- Regulatory and legal experience helps navigate evolving digital asset regulation across multiple jurisdictions and compliance frameworks

Traditional finance skills alone are not enough; understanding digital assets is also important. A director with many years of hedge fund experience but no knowledge of custody security, smart contract risks, or DeFi protocols cannot effectively oversee digital assets. On the other hand, someone with only crypto experience and no understanding of institutional rules may miss important aspects like governance, regulations, and operational procedures.

1.1.2 COMMITTEE STRUCTURE BY FIRM SIZE

Committee formation must match the company's growth and complexity. Creating committees too early can cause unnecessary bureaucracy, while waiting too long can result in oversight gaps. Proper timing ensures effective governance and oversight in digital asset investments.

TABLE 1: COMMITTEE STRUCTURE BY AUM LEVEL

AUM Level	Committee Requirements
Below $50M	Complete board oversight without formal committees. Board reviews financial statements, operational metrics, and compliance reports directly.
$50M - $100M	Establish an Audit Committee (minimum two independent directors) for financial reporting oversight, external audit coordination, internal control assessment, and compliance program review.
$100M - $250M	Add a Risk Committee (minimum two directors, at least one independent) to oversee the risk appetite framework, limit monitoring, stress testing, and technology risk oversight.
Above $250M	Consider nominating and governance committees for board composition, executive compensation, succession planning, and evolution of the governance framework.

1.1.3 MEETING CADENCE AND DOCUMENTATION

Effective board meetings are essential for good oversight and operational efficiency. For investment portfolios under $50 million in assets under management (AUM), hold quarterly board meetings and provide monthly written updates. These updates should include performance data, compliance status, and operational metrics. For portfolios between $50 million and $250 million, increase the frequency to quarterly board meetings and add monthly committee meetings to review specific areas in detail. For portfolios exceeding $250 million, conduct monthly board meetings to manage the increased complexity and meet institutional expectations. This structure ensures proper oversight while maintaining operational efficiency across different asset sizes.

Every board meeting should address:

- Management performance update covering financial results, operational KPIs, key hires and departures, and strategic initiative progress
- Investment performance analysis with detailed risk metrics, including VaR, drawdown analysis, concentration limits, and performance attribution
- Compliance and regulatory updates detailing rule changes, examination activity, violation logs, and remediation status

- Technology and security status reviewing infrastructure changes, security incidents, vulnerability assessments, and disaster recovery testing
- Strategic initiative tracking covering new product development, fundraising activity, service provider changes, and material partnerships
- Executive session conducted without management present to discuss executive performance, compensation, succession planning, and any concerns

Clear documentation is essential for effective governance. Always distribute detailed board packages five to seven days before meetings. These should include performance reports, risk dashboards, compliance updates, and financial statements. Meeting minutes must record who attended, key discussions, all decisions with reasons, any dissenting opinions, and action items with assigned owners and deadlines. Follow up on action items to ensure completion and report progress at future meetings. Poor documentation undermines governance and suggests superficial oversight rather than genuine management.

> Most fiduciary breakdowns in digital asset funds stem not from strategy failure but from concentrated authority. No oversight model can function effectively when one person controls trading, custody, and cash movement. Boards that meet infrequently or lack digital asset expertise cannot provide meaningful oversight of protocol risks, smart contract vulnerabilities, or custody architecture. A best practice is ensuring at least one board member can engage substantively on digital asset operations—not just investment thesis, but custody mechanics, key management, and protocol-level risks. During diligence, allocators often assess whether directors can articulate specific digital asset risks without deferring entirely to management. Generic board credentials without crypto-specific knowledge yield governance in name only.

1.2 MANAGEMENT STRUCTURE AND ACCOUNTABILITY

The management structure of an organization is crucial in determining how effectively it can grow and adapt. A well-designed structure ensures that operations can expand systematically, rather than relying heavily on specific individuals. When leadership roles such as CEO and CIO are combined with operational control, it creates a significant risk. This setup can lead to a single point of failure, affecting strategy, execution, and risk management. For institutional investors, this is a concern because they prefer to invest in firms where authority is balanced.

Clear checks and balances are essential to ensure accountability and reduce risks. Therefore, investment managers should prioritize organizations with transparent and balanced management structures to safeguard their investments and promote sustainable growth.

1.2.1 CORE LEADERSHIP ROLES

The executive leadership structure should focus on four leading roles, each bearing unique responsibilities essential for organizational success. These roles need not all be filled immediately at launch, but firms must demonstrate clear progression toward complete separation as assets and complexity grow.

- *Chief Executive Officer (CEO):* The CEO is ultimately responsible for the firm's strategy, business development, capital raising, board relations, and organizational culture. This role focuses externally on growth while ensuring internal resources align with strategic priorities. The CEO should not control day-to-day investment decisions or operational execution—concentrating strategic and tactical authority eliminates the necessary tension between growth ambitions and risk management.
- *Chief Investment Officer (CIO):* The CIO directs investment strategy, portfolio construction, and investment team management. Responsibilities include strategy development, risk budget allocation, leadership of the investment committee, oversight of the research process, and performance analysis. The CIO should not have unilateral trade execution authority, custody control, or operational oversight—separating investment authority from operational execution creates an essential control structure.
- *Chief Operating Officer (COO):* The COO manages operational infrastructure, service provider relationships, and business operations. This includes trade operations, reconciliations, fund administration coordination, valuation processes, investor reporting, and technology oversight. The COO provides independent verification of investment activities and ensures operational controls function effectively. In emerging firms, a strong operations professional with segregation from investment authority proves more valuable than a CEO-CIO who also manages operations.
- *Chief Compliance Officer (CCO):* The CCO designs, implements, and monitors the compliance program. This role requires independence from investment and operational pressures—reporting directly to the board or CEO rather than the CIO. Responsibilities include regulatory filing management, policy development and enforcement, examination coordination, violation investigation, and remediation oversight. The CCO cannot report to the person whose activities

require monitoring—structural independence enables effective compliance oversight.

1.2.2 SCALING LEADERSHIP AS FIRMS GROW

The leadership structure should evolve as the firm expands, gradually assigning responsibilities to avoid conflicts of interest. The pace of this development depends on asset growth, the complexity of strategies, and investor requirements. For institutional investors, it is important to demonstrate clear progress toward fully separating roles to ensure transparency and accountability.

TABLE 2: LEADERSHIP TEAM STRUCTURE

Stage	Management Structure
Launch to $25M	The founder serves as CEO-CIO with an external CCO (consultant or fractional). Hire a senior operations professional or outsource to a fund administrator. Essential separation: the founder cannot have sole custody or control.
$25M to $100M	Separate the CEO and CIO roles, OR hire a full-time COO. Bring CCO in-house. Establish an Investment Committee with external members. Critical separation: different individuals control investment decisions and trade execution.
$100M to $250M	Complete separation of the CEO, CIO, COO, and CCO roles. Add Chief Technology Officer if technology is a core competency. Build a middle management layer with clear reporting relationships. Establish a Risk Committee with independent oversight.
Above $250M	Full C-suite with specialized roles (CFO, CTO, Head of Risk). Distributed authority with documented approval hierarchies. Multiple layers of review for material decisions. Professional management structure independent of founders.

1.2.3 ORGANIZATIONAL DESIGN PRINCIPLES

Effective organizational design should include clear reporting lines, delegated authority, and proper documentation. The following principles provide guidance on structuring organizations, regardless of their size:

- *No individual controls investment decisions and operational execution:* The person making investment decisions should not also execute trades, control custody, or manage cash operations. This separation creates natural verification points and eliminates single-point fraud risk.
- *Clear escalation hierarchies for exceptions:* Document who can approve exceptions to policies, limits, and standard procedures. CEO discretion to override controls eliminates the value of those controls. Material exceptions require board notification or approval, depending on significance.
- *Written position descriptions with approval authorities:* Every role should have documented responsibilities and approval limits. Vague authorities create confusion during operational stress. Clear documentation enables succession planning and training.
- *Segregation of duties for critical functions:* Separate individuals should initiate transactions, approve transactions, and reconcile results. The same person cannot perform trade initiation, custody control, and reconciliation without independent verification.
- *Independent compliance and risk functions:* Compliance and risk management require independence from business pressures. These functions report to the board or the CEO—never to the individuals whose activities they monitor. Performance incentives should not conflict with control effectiveness.

A primary management failure is the founder-CEO-CIO who also controls operations and technology, creating a single point of failure across decision-making, execution, and risk management. Institutional allocators are unlikely to invest where one person makes investment decisions, executes trades, controls custody, and manages cash without independent oversight. Best practice is establishing clear segregation even at small scale—if full role separation isn't feasible, ensure no single individual can complete critical processes (especially asset movements) without independent verification. A common diligence question is: "If your CIO is unavailable for 30 days, who specifically performs each of their critical functions?" Having documented answers with named individuals and written authority demonstrates operational maturity.

1.3 POLICY FRAMEWORK AND DOCUMENTATION

Policies turn governance principles into clear operational steps. Good policies should specify what actions are needed, who is responsible, how often controls should be checked, what records show compliance, and who can approve exceptions. Vague policies that only say the firm 'maintains appropriate controls' do not give clear guidance or accountability if controls are not effective.

1.3.1 CORE POLICY ARCHITECTURE

Your policy framework should cover all key operational areas with enough detail to guide actions. The main policies for managing institutional-grade operations include:

- *Compliance Policy and Procedures Manual:* Comprehensive document covering regulatory obligations, supervision procedures, recordkeeping requirements, and compliance testing. Must be reviewed and updated annually with board approval. This serves as your operational rulebook for regulatory adherence.
- *Code of Ethics:* Governs personal trading, conflicts of interest, gifts and entertainment, outside activities, and confidential information. Digital asset-specific provisions must address token holdings, DeFi participation, protocol contributions, and governance voting. All access persons must acknowledge annually.
- *Investment Policy Statement:* Defines investment objectives, strategy parameters, risk limits, eligible instruments, concentration limits, leverage constraints, and prohibited transactions. Must be specific enough to constrain discretion while flexible enough to execute strategy. Generic language like 'invest in digital assets' provides no meaningful constraint.
- *Valuation Policy:* Establishes pricing hierarchy, source prioritization, committee processes for complex assets, and escalation procedures for pricing disputes. Digital assets require specific guidance for illiquid tokens, DeFi positions, staking derivatives, and protocol-specific instruments.
- *Business Continuity and Disaster Recovery:* Details procedures for operational disruptions, key-person unavailability, technology failures, and security incidents. Must address custody key recovery, multi-signature procedures, service provider failures, and communication protocols. Regular testing is required with documented results.
- *Custody and Security Policy:* Defines custody models, authorization procedures, key management protocols, multi-signature requirements, hot/cold wallet

allocations, and security reviews. Digital asset custody requires explicit operational procedures—generic references to 'industry standard security' prove insufficient.

- *Risk Management Policy:* Establishes risk appetite framework, limit structure, monitoring procedures, escalation processes, and breach protocols. Must address traditional risks (market, credit, liquidity, operational) and digital-asset specific risks (smart contract, protocol, custody, blockchain).

1.3.2 IMPLEMENTATION AND EXCEPTION MANAGEMENT

Policies provide value only when implemented and enforced. The gap between written policies and actual practice destroys credibility with allocators and creates regulatory liability without offering protection.

Implementation Requirements:

- *Training and acknowledgment:* All employees must receive training on relevant policies and acknowledge understanding annually. Maintain training completion records and attestations.
- *Monitoring and testing:* Establish systematic testing procedures to verify policy compliance. Document testing methodology, frequency, sample sizes, findings, and remediation.
- *Violation procedures:* Investigate policy violations promptly, document findings, impose appropriate discipline, and implement corrective measures. Maintain violation logs showing issue identification, investigation, and resolution.
- *Regular review and updates:* Review policies annually or when business changes materially. Document review dates, changes made, and approval. Policies unchanged for years signal disconnection from actual operations.

Policies that exist only on paper create liability without providing protection. The gap between documented procedures and actual practice erodes credibility faster than having acknowledged informal processes. Allocators typically test policy effectiveness by requesting exception logs, training records, testing reports, and violation documentation. A useful self-assessment: "Can we walk through a recent policy exception—what was requested, who approved it, what was the business rationale, and how was it documented?" Firms unable to provide specific examples may signal that policies are aspirational rather than operational. Notably, having zero exceptions over extended periods can itself raise questions—either monitoring may be insufficient, or the policy framework may be disconnected from actual operations.

1.4 SUCCESSION PLANNING AND KEY PERSON RISK

Succession planning addresses what happens when critical personnel become unavailable—through departure, incapacitation, or death. Digital asset firms face acute key-person risk because specialized knowledge often concentrates among founding team members. The CIO, who is the only person understanding the firm's DeFi strategy, creates existential risk. The COO, who is the only person with custody access, creates operational risk. Allocators assess succession planning not through aspirational documents but through specific answers to the question: 'If this person is unavailable for 30 days, who performs their responsibilities and what documentation enables continuity?'

1.4.1 CRITICAL ROLE COVERAGE REQUIREMENTS

Identify roles where unavailability would materially disrupt operations, investment management, or regulatory compliance. For each critical role, document:

- *Primary successor:* Specific individual who assumes responsibilities during short-term absence (internal or board member for small firms)
- *Knowledge documentation:* Written procedures covering critical processes, system access requirements, key relationships, and decision frameworks
- *Access procedures:* Methods for accessing systems, accounts, and information if the critical person becomes unavailable unexpectedly
- *Cross-training evidence:* Documentation that successors have performed critical functions, understand procedures, and can execute independently

- *Long-term succession strategy:* Recruitment pipeline, internal development programs, or board-approved interim leadership for permanent departures

---

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional investors assess governance based on what firms can show, not just what they say. Vague answers suggest governance is only on paper, not practiced. They should check if the firm's board challenges management to ensure independence. They should also evaluate if directors have the expertise to understand digital asset risks. Additionally, they should review whether governance practices have effectively prevented issues or simply documented problems after they occurred. Firms that cannot provide clear examples, respond quickly to documentation requests, or explain their governance decisions may indicate operational immaturity. This approach helps ensure that governance is genuine and effective in managing digital assets, aligning with best practices for fiduciary responsibility.

Board Independence and Expertise

- How many directors are genuinely independent—no material financial relationships, family connections, or economic dependence on the firm?
- What specific digital asset operational experience does each director possess? Traditional finance credentials alone prove insufficient.
- Provide board meeting minutes from the past four quarters showing attendance, discussion depth, and challenges to management proposals.
- Describe a specific instance where the board rejected or significantly modified a management recommendation. Inability to provide examples signals rubber-stamp oversight.
- How does the board oversee custody security, smart contract risks, and protocol vulnerabilities? Generic "we monitor risks" responses fail scrutiny.

Management Structure and Accountability

- Walk through the background and track record of each C-suite executive. What relevant failures or successes preceded their current role?
- Who can execute trades, authorize custody movements, and override compliance controls? Concentration in one person disqualifies institutional capital.
- What happens operationally if the CIO is unavailable for 30 days? Inability to answer specifically reveals key person dependency.

- How is executive compensation structured? Short-term incentives without meaningful deferrals signal misalignment with long-term fiduciary obligations.
- Provide your organizational chart showing reporting relationships and segregation of duties. Circular reporting or unclear authorities indicate structural deficiencies.

Policy Effectiveness and Enforcement

- Describe a recent policy exception—what was requested, who approved it, what was the business rationale, and how was it documented? Zero exceptions over extended periods suggest either inadequate monitoring or policies routinely ignored.
- How do you verify policies reflect actual operations rather than aspirational frameworks? Testing records and violation logs reveal the gap between documentation and reality.
- Provide training records and attestations for the past year. Incomplete records signal policies exist without implementation.
- Walk through how a specific policy evolved as your business changed. Static policies unchanged for years indicate governance disconnected from operations.
- Who has the authority to approve policy exceptions for different categories? Unlimited CEO discretion or unclear approval hierarchies reveal inadequate controls.

Documentary Evidence Requirements

- Board meeting minutes for the past four quarters with attendance records, key discussions, votes, and action items
- Current organizational chart showing all reporting relationships and segregation of duties
- Complete policy library with version control, revision dates, and approval documentation
- Training completion records and employee attestations for the past 12 months
- Exception logs with requests, approvals, rationales, and remediation tracking
- Succession plans with documented processes and backup coverage for critical roles

COMMON PITFALLS AND REMEDIATION

- *Board lacks independence or digital asset expertise*. Directors with no operational crypto knowledge defer to management on custody, protocol, and smart contract matters—providing oversight in name only. Remediation: Recruit at least one director with hands-on digital asset operational experience (not just investment exposure). Define minimum meeting attendance and require documented challenge in minutes.
- *Founder concentrates CEO, CIO, and operational authority*. One person controls investment decisions, trade execution, custody, and cash movement without independent verification. Remediation: Separate investment authority from operational execution. If full role separation isn't feasible, require dual authorization for all asset movements and establish a board committee with direct operational oversight.
- *Policies exist but aren't enforced*. Written procedures don't match actual practice—no training records, no testing, no exception logs. Remediation: Implement annual training with documented attestations, quarterly compliance testing with written findings, and exception logs capturing every deviation with approval and rationale.
- *Committees approve without deliberation*. Meeting minutes show unanimous approval of all proposals with no recorded discussion or challenge. Remediation: Require charters specifying committee authority to reject or modify proposals. Include at least one independent member. Minutes must document questions raised and rationale for decisions—not just outcomes.
- *No succession coverage for critical roles*. Key person departure would leave no one able to perform essential functions—custody access, strategy execution, regulatory filings. Remediation: Identify critical roles, name specific successors, document procedures enabling handover, and test succession annually by having backups perform functions.
- *Governance documents are static*. Policies and org charts unchanged for years despite business evolution—new strategies, personnel, service providers. Remediation: Establish annual governance review with board sign-off. Maintain version control showing revision history. Update within 30 days of material changes.

KEY CONTROLS & DOCUMENTATION

Document	Purpose	Update Frequency	Owner
Board Charter	Defines board authority, responsibilities, and procedures	Annual	Corporate Secretary
Committee Charters	Outlines committee scope, composition, and authority	Annual	Committee Chairs
Organizational Chart	Shows reporting relationships and structure	Quarterly	CEO
Delegation of Authority	Specifies who can make what decisions	Semi-annual	COO
Role Descriptions	Details responsibilities and required qualifications	Annual	HR/COO
Succession Plans	Identifies backup coverage for key positions	Semi-annual	CEO
Policy Library	Complete set of operational policies	Annual	CCO
Meeting Minutes	Records board and committee decisions	Per meeting	Secretary
Training Records	Documents policy training and attestations	Ongoing	CCO
Exception Log	Tracks policy exceptions and resolutions	Monthly	CCO

STANDARD 2: REGULATORY COMPLIANCE

Firms must maintain robust compliance programs. This includes an independent compliance function with appropriate resources, authority, and reporting lines; a comprehensive compliance program addressing all applicable laws, rules, and regulations across jurisdictions; and proactive monitoring of regulatory developments and their impact on firm operations. Firms must implement robust Anti-Money Laundering (AML) and Know Your Customer (KYC) procedures appropriate to their investor base and establish a framework for managing multi-jurisdictional compliance obligations.

Regulatory rules for digital assets are still not clear and are not fully established. Unlike traditional assets, which have well-defined laws and regulations, digital assets raise many questions about which rules apply and which authorities are responsible. Often, rules designed for other asset types are used for tokens, but this can lead to confusion. This uncertainty does not mean firms can ignore compliance; instead, it highlights the importance of adhering to good practices. Firms that operate without proper registration may find it difficult to attract institutional investors, regardless of the quality of their operations or investments.

Standard 2 highlights that firms should have strong compliance programs, even when regulations are uncertain. They should ensure they are registered with the appropriate authorities and keep detailed records of their activities. It is also important to have systems in place to monitor and regularly test compliance. If issues arise, firms should respond promptly and document how they address and resolve these problems. Failing to maintain proper compliance can lead to legal penalties, operational challenges, and damage to the firm's reputation.

To meet this standard, firms should view compliance as a fundamental part of their operations, not just a legal obligation. They should employ experienced compliance staff who understand both traditional finance and digital assets. Utilizing technology to monitor compliance effectively can be beneficial. Maintaining detailed records of all compliance activities is essential. Firms should also ensure that their compliance functions operate independently and are not influenced by business pressures. Compliance should be integrated into risk management and trust-building efforts with investors, rather than treated as a mere formality or checkbox exercise.

2.1 REGULATORY REGISTRATION AND LICENSING

Registration is the cost of accessing institutional capital. Operating without necessary licenses immediately disqualifies you from institutional investment regardless of operational quality. Digital asset firms often activate multiple regulatory regimes simultaneously—investment adviser registration, commodity trading advisor registration, money transmitter licenses, and foreign registrations. Each regime brings distinct obligations, examination risk, and operational requirements.

2.1.1 SEC INVESTMENT ADVISER REGISTRATION

The Securities and Exchange Commission (SEC) registration threshold is $100 million in Regulatory Assets Under Management. Crossing this threshold brings federal jurisdiction, requiring Form ADV filing and SEC examination oversight. Below this level, state registration applies, with each jurisdiction having distinct requirements. Most institutional allocators require federal registration regardless of AUM level—state-registered advisers face higher scrutiny and limited capital access.

Form ADV Requirements:

- *Form ADV Part 1:* Detailed disclosure of business operations, ownership structure, disciplinary history, custody arrangements, conflicts of interest, and affiliated entities. Digital asset advisers must disclose token custody models, counterparty relationships with exchanges, and DeFi protocol exposures.
- *Form ADV Part 2:* Client disclosure brochure written in plain English describing services offered, fee structures, conflicts of interest, disciplinary information, custody practices, and material risks. Digital asset sections must address custody security, smart contract risks, protocol vulnerabilities, exchange counterparty risk, and regulatory uncertainty affecting client investments.
- *Digital Asset-Specific Disclosures:* Must explicitly address: private key management and custody architecture, exchange failure and counterparty risk, smart contract vulnerabilities and audit limitations, DeFi protocol risks and governance participation, illiquidity in volatile markets, regulatory classification uncertainty, and potential for complete loss.

Annual amendments are required within 90 days of the fiscal year-end. Material changes require prompt amendments—new custody relationships, disciplinary actions, or ownership changes trigger immediate filing obligations. Failure to maintain the current Form ADV creates examination findings and allocator concerns about operational rigor.

2.1.2 CFTC AND NFA REGISTRATION

Engaging in trading cryptocurrencies like Bitcoin or Ethereum involves specific rules set by the Commodity Futures Trading Commission (CFTC). The CFTC considers both Bitcoin and Ethereum as commodities. This means that trading futures for these cryptocurrencies must follow certain regulations. Traders need to become members of the National Futures Association (NFA) and must register as either a Commodity Trading Advisor (CTA) or a Commodity Pool Operator (CPO). These rules are in place to make the market transparent, protect investors, and keep the market fair, especially as digital assets become more popular and widespread.

CTA Registration Requirements:

- All principals must pass the Series 3 exam, demonstrating commodity trading knowledge
- Disclosure documents must be filed with NFA separately from Form ADV, addressing commodity-specific risks
- Monthly reports must be submitted to NFA detailing assets under management and positions
- Separate books and records must be maintained for commodity accounts with specific retention requirements

CPO Registration Requirements:

Operating pooled investment funds that trade commodity futures requires registration as a Commodity Pool Operator (CPO). This registration involves stricter rules compared to becoming a Commodity Trading Advisor (CTA). CPOs must prepare annual financial reports that are audited and follow either US GAAP or IFRS standards. They also need to send quarterly account statements to investors to keep them informed about fund performance. CPOs must use specific methods to report performance consistently across reports. Protecting client assets is essential, so customer funds must be kept separate at registered futures commission merchants (FCMs). Good recordkeeping is also necessary to meet regulatory requirements and support audits. Overall, becoming a CPO involves higher costs and more operational work than just registering as an investment adviser. This is because of the increased rules and protections designed to safeguard investors when trading commodity futures through pooled funds.

2.1.3 MONEY TRANSMITTER LICENSING

The rules for money transmitters are complex and vary widely across different regions. Each jurisdiction sets its own standards for what counts as money transmission, creating a fragmented regulatory environment. This situation increases compliance challenges for businesses operating in multiple areas. Typical activities that may trigger regulatory

requirements include holding private keys for customer assets, enabling exchanges between fiat currencies and cryptocurrencies, managing omnibus wallet structures, and offering custody services that involve control over customer assets. This patchwork of regulations makes compliance more difficult and highlights the need for clearer, more consistent frameworks. Such frameworks are essential to support the sustainable growth and stability of the digital asset industry, providing a reliable foundation for investment managers and other industry participants.

Federal Level Requirements:

Registration with the Financial Crimes Enforcement Network (FinCEN) as a Money Services Business (MSB) is required for most digital asset activities like sending, exchanging, and storing digital currencies. This registration involves following certain rules to prevent illegal activities. These rules include setting up a Customer Identification Program (CIP) to verify customer identities, filing Suspicious Activity Reports (SARs) to report suspicious transactions, and Currency Transaction Reports (CTRs) for transactions over $10,000. Companies must also have an Anti-Money Laundering (AML) program to detect and prevent money laundering and related crimes. Following these rules is important for legal reasons and helps keep the digital asset industry transparent. It also reduces the chances of financial crimes and supports the integrity of the financial system.

State-by-State Licensing:

State requirements for licensing money transmitters differ significantly. In New York, the BitLicense is very strict, requiring firms to meet capital standards, implement comprehensive compliance and cybersecurity programs, establish anti-money laundering procedures, undergo examinations, and cover high application costs. Other states may exempt certain activities or offer simpler licensing processes. Activities that require licensing in New York might be exempt in Montana or Wyoming. Investment firms should analyze the licensing requirements in each state where they have clients or operations. Operating without the necessary state licenses can lead to criminal liability and regulatory penalties, emphasizing the importance of understanding and complying with each state's regulations.

TABLE 1: U.S. REGISTRATION MATRIX

Registration Type	Key Obligations
SEC Investment Adviser	Form ADV filing and annual amendments; compliance manual and annual review; Code of Ethics; custody rule compliance if holding client assets; books and records retention; examination readiness.

Registration Type	Key Obligations
CFTC/NFA CTA	Series 3 exam for principals; NFA membership; separate disclosure document; monthly reporting to NFA; separate books and records; NFA examination authority.
CFTC/NFA CPO	All CTA requirements plus: annual audited financials; quarterly account statements to participants; segregated customer funds; enhanced performance reporting; higher capital requirements.
FinCEN MSB	MSB registration; Customer Identification Program; SAR filing procedures; CTR filing for large transactions; comprehensive AML program; Travel Rule compliance for crypto transfers.
State Money Transmitter	State-specific requirements varying by jurisdiction; surety bonds or capital requirements; regular financial reporting; state examination authority; annual license renewals; potential for multi-state licensing.

2.1.4 INTERNATIONAL REGISTRATION REQUIREMENTS

International operations trigger additional registration obligations. Accepting non-US investors, operating offshore funds, or maintaining non-US offices each creates distinct registration requirements:

- *European Union:* MiFID II (Markets in Financial Instruments Directive) applies to investment services across member states. Digital asset services may require authorization as an Alternative Investment Fund Manager or Crypto-Asset Service Provider under MiCA (Markets in Crypto-Assets Regulation) beginning 2024.
- *United Kingdom:* Financial Conduct Authority (FCA) authorization required for UK operations. Crypto asset firms require registration under Money Laundering Regulations. Post-Brexit, UK regulation diverges from EU requirements.
- *Cayman Islands:* Cayman Islands Monetary Authority (CIMA) registration applies to fund managers. Most offshore hedge funds domicile in Cayman, requiring CIMA registration for the management company and fund licensing.
- *Singapore:* Monetary Authority of Singapore (MAS) licensing covers digital payment token services. Singapore's progressive framework makes it attractive for Asian operations but requires significant compliance infrastructure.

- *Switzerland:* FINMA (Swiss Financial Market Supervisory Authority) regulates fund management and crypto service providers. Switzerland's 'Crypto Valley' offers favorable regulatory treatment but requires local presence and capital requirements.

A common registration gap is assuming one license covers all activities. SEC investment adviser registration does not authorize futures trading (requiring CFTC/NFA registration), custody operations may trigger state money transmitter requirements, and non-US investors often require foreign registrations. Each business activity warrants analysis against applicable registration triggers. Best practice is maintaining a registration matrix that maps each activity to its regulatory requirements, with supporting legal analysis. This should be reviewed whenever the business model evolves. Vague references to "appropriate registration" without documented analysis of specific activities—trading, custody, investor geography—may not withstand regulatory scrutiny or allocator diligence.

2.2 COMPLIANCE PROGRAM ARCHITECTURE

A compliance program acts as a system for ensuring adherence to regulations. In digital assets, it should cover traditional issues such as insider trading and best execution, as well as new challenges like governance participation in decentralized finance, risk assessment of smart contracts, and monitoring on-chain transactions. Institutional investors evaluate the effectiveness of their programs through testing records, violation logs, and remediation documentation, rather than relying solely on policy documents.

2.2.1 CHIEF COMPLIANCE OFFICER INDEPENDENCE

The Chief Compliance Officer (CCO) role requires specialized expertise and true independence. The CCO cannot effectively monitor activities while reporting to individuals whose conduct requires oversight. Essential independence elements include:

- *Direct reporting to CEO or Board:* CCO must not report to CIO, COO, or other operational leaders whose activities require monitoring. Direct board access enables escalation without management filtering.
- *Protected budget authority:* CCO controls compliance budget without requiring approval from individuals whose activities generate compliance costs. Inability

to retain counsel or implement monitoring tools without business unit approval eliminates independence.

- *Authority to halt violations:* CCO must have clear authority to stop activities violating policies or regulations without requiring approval. Trading restrictions, marketing holds, or operational changes should not require business unit consent.
- *Termination protections:* CCO termination should require board notification if not board approval. Management's ability to remove CCO without board oversight eliminates independence when compliance challenges business priorities.

The CCO must possess both traditional compliance experience from SEC, CFTC, or FINRA backgrounds and digital asset knowledge including smart contracts, DeFi protocols, and blockchain technology. Generalist compliance professionals without crypto-specific expertise cannot assess protocol risks, custody vulnerabilities, or on-chain transaction patterns. Conversely, crypto-native personnel without traditional compliance backgrounds lack understanding of fiduciary obligations, insider trading rules, and examination procedures.

Firms with AUM below $100 million often use fractional or consulting CCOs. This model functions effectively if the consultant has sufficient time allocation, direct board access, and independence from management. Part-time arrangements with inadequate hours, limited access, or reporting through operational management create appearance of compliance without substance.

2.2.2 COMPLIANCE MANUAL STRUCTURE

Your compliance manual covers both traditional and digital asset requirements. Generic templates are ineffective because they include language that does not match actual operations. The manual should include clear operational procedures that employees can follow, rather than just aspirational statements about compliance culture. It is important that the manual provides practical guidance tailored to the specific processes involved in managing digital assets, ensuring that all team members understand their responsibilities and actions required to maintain compliance effectively. This approach supports the fiduciary standards set by the governing board for investment management in the digital asset space, aligning operational practices with regulatory expectations and best practices in the industry.

Core Manual Components:

- *Regulatory framework:* Documents all applicable regulations including SEC, CFTC, state, and international requirements. Identifies specific rule obligations and implementation procedures.
- *Personal trading controls*: Specifies pre-clearance procedures, restricted lists, holding periods, and reporting requirements. Digital asset provisions must address token holdings, DeFi positions, staking, and governance participation.
- *Conflicts of interest:* Identifies potential conflicts specific to digital assets including protocol investments, service provider relationships, token allocations, and affiliate transactions. Establishes disclosure and mitigation procedures.
- *Best execution:* Establishes trade routing procedures, counterparty selection criteria, execution quality monitoring, and documentation requirements. Addresses digital asset-specific factors including exchange liquidity, custody arrangements, and settlement risk.
- *Marketing and advertising*: Governs all client communications including performance advertising, social media, conference presentations, and pitch materials. Requires compliance review before distribution.
- *Books and records:* Specifies retention requirements for all regulatory documents, client communications, trading records, and compliance testing. Digital preservation with immutable timestamps required.
- *Supervision procedures:* Establishes monitoring procedures for all supervised persons including investment team, operations, and business development. Frequency, scope, and documentation requirements specified.

2.2.3 ANNUAL COMPLIANCE REVIEW

SEC Rule 206(4)-7 requires annual compliance program review assessing adequacy and effectiveness. This is not a checkbox exercise—it requires systematic evaluation of whether procedures prevented violations, testing identified issues, and remediation addressed problems. The annual review should examine:

- *Changes in business activities:* New strategies, service providers, custody arrangements, or client types that require policy updates or additional controls.
- *Testing results:* Analysis of all compliance testing performed during the year, violations identified, root causes, and remediation effectiveness.
- *Regulatory developments:* New rules, guidance, examination findings, or enforcement actions requiring policy or procedure changes.

- *Technology changes:* New systems, platforms, or tools affecting recordkeeping, supervision, or control effectiveness.
- *Adequacy assessment:* Whether current procedures address all material risks, cover all supervised activities, and enable effective monitoring.

The annual review should be documented in writing and presented to senior management and the board. It should lead to specific plans for fixing any identified issues. Generic reviews that only state that policies are adequate, without analyzing testing results, violations, or areas needing improvement, indicate a focus on appearance rather than effective oversight.

> Compliance programs commonly fail in two ways: the CCO lacks genuine independence, or the CCO lacks digital asset expertise. A CCO reporting to the CIO may face challenges objectively monitoring investment activities. A CCO without blockchain knowledge may struggle to assess protocol risks or interpret on-chain transaction patterns effectively. Best practice is ensuring the CCO has both structural independence (reporting to CEO or board, with direct board access) and substantive expertise (understanding of custody mechanics, DeFi protocols, and blockchain analytics). Allocators often evaluate compliance through testing evidence—methodology, samples, findings, and remediation—rather than manual quality alone. Well-documented testing work papers demonstrate that compliance is operational, not just documented.

2.3 ANTI-MONEY LAUNDERING PROGRAM

Anti-money laundering obligations in digital assets are more extensive than in traditional finance because of features such as pseudonymous transactions, cross-border transfers without intermediaries, mixing services that hide transaction history, and regulatory arbitrage across different jurisdictions. Investment managers who accept clients or trade on exchanges become part of the financial system and are expected to comply with anti-money laundering regulations. Institutional allocators evaluate anti-money laundering programs by examining on-chain monitoring capabilities, sanctions screening procedures, and the implementation of the Travel Rule. These measures are important even beyond the basic Know Your Customer (KYC) documentation, ensuring comprehensive compliance and risk management in digital asset activities.

2.3.1 CUSTOMER DUE DILIGENCE FRAMEWORK

Customer Identification Program requirements are relevant for all money services businesses and many digital asset firms. Enhanced due diligence is necessary for higher-risk customers, including foreign investors, politically exposed persons, entities with complex ownership structures, and customers from high-risk jurisdictions. Investment managers in the digital asset space should adhere to these guidelines to ensure compliance and maintain integrity in fiduciary responsibilities. Proper identification and thorough review of clients from high-risk categories are essential to prevent financial crimes and uphold regulatory standards. It is important to follow these procedures diligently to support transparency and accountability within the industry.

Standard KYC Collection:

- Legal name and date of birth with government-issued identification verification
- Residential address verification through utility bills, bank statements, or government documents
- Tax identification number (SSN for US persons, TIN for entities)
- Source of funds and source of wealth for high-risk investors
- Beneficial ownership information for entities (FinCEN CDD Rule)

Digital Asset-Specific Enhanced Due Diligence:

- Wallet address disclosure for direct blockchain transactions
- On-chain transaction history analysis using blockchain analytics tools
- Exchange account verification and source of crypto assets
- Screening for connections to mixing services, darknet markets, or sanctioned addresses
- Geographic risk assessment for cross-border crypto transfers

2.3.2 TRANSACTION MONITORING AND RED FLAGS

Ongoing transaction monitoring identifies suspicious activity requiring Suspicious Activity Report (SAR) filing. Digital asset monitoring requires both traditional pattern analysis and on-chain surveillance. Red flags specific to digital assets include:

- Deposits from mixing services or privacy coins suggesting transaction history obfuscation
- Rapid movement through multiple wallets without economic purpose

- Structuring to avoid reporting thresholds or regulatory attention
- Activity inconsistent with stated investment purpose or client profile
- Connections to addresses on sanctions lists or known illicit actors

---

2.4 MARKETING AND INVESTOR COMMUNICATIONS

Marketing violations in digital assets often involve performance presentation rather than fraudulent claims. Common errors include: showing returns for a single account rather than a composite, cherry-picking favorable time periods, using gross returns without fee disclosure, comparing to inappropriate benchmarks, and making forward-looking statements without adequate risk disclosure. Securities law treats all investor communications as 'advertising' requiring compliance review—this includes pitch decks, newsletters, social media, conference presentations, and website content.

2.4.1 SECURITIES LAW FRAMEWORK

Rules from the SEC prohibit false or misleading statements in advertising. They require fair presentation of important facts and specific disclosures. When marketing digital assets, it is important to address issues such as the regulatory classification of tokens, risks related to custody and security, the potential for illiquidity in volatile markets, the possibility of total loss, and conflicts of interest. Generic disclaimers about cryptocurrency volatility are not enough. Clear and detailed disclosures about specific risks are necessary to support informed investment decisions.

Required Content Standards:

- *No misleading statements:* All material facts presented fairly without omission. Half-truths or misleading implications violate advertising rules even if individual statements are technically accurate.
- *Performance presentation:* Must use composites rather than cherry-picked accounts. Gross and net returns clearly distinguished. Time periods representative, not selected for favorable results.
- *Risk disclosure:* Material risks disclosed prominently, not buried in footnotes. Digital asset-specific risks including custody, regulatory, smart contract, and market risks addressed specifically.
- *Fee disclosure:* All direct and indirect fees disclosed. Management fees, performance fees, fund-level expenses, and trading costs clearly presented.

- *Compliance approval:* All marketing materials reviewed and approved by CCO before distribution. Documentation of approval maintained.

2.5 REGULATORY EXAMINATIONS

Regulatory examinations test whether operations match disclosures and policies match practice. SEC exams focus on: Form ADV accuracy, custody rule compliance, fee calculation accuracy, conflicts disclosure, marketing rule adherence, and books and records completeness. CFTC/NFA exams emphasize: segregation of customer funds, disclosure document accuracy, performance calculations, and recordkeeping. The most damaging examination finding is not a substantive violation but rather inability to produce requested documents—this signals systematic control failures.

2.5.1 EXAMINATION READINESS

Examination readiness requires systematic document management enabling prompt production of any requested record. Organizations should maintain:

- *Centralized document repository:* All policies, procedures, testing records, training materials, and compliance documentation organized and readily accessible.
- *Trade authorization records:* Documentation showing investment decision rationale, approval process, execution instructions, and best execution analysis.
- *Marketing materials archive:* All presentations, pitch decks, performance reports, website content, and social media posts with compliance approval documentation.
- *Client communications:* All correspondence, meeting notes, advisory agreements, and disclosure documents.
- *Testing work papers:* All compliance testing performed including methodology, sample selection, findings, and remediation.

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional allocators assess compliance by testing how well programs operate under real-world conditions, rather than just reviewing polished manuals. They can tell the difference

between firms with genuine compliance systems and those that only maintain paperwork to meet minimum standards. If a firm cannot produce testing reports, explain specific violations, or show systematic steps taken to fix issues, it indicates that compliance is more of an aspiration than an operational reality.

Registration Completeness

- Provide current Form ADV Parts 1 and 2A with all amendments. Outdated filings signal inadequate regulatory attention.
- What registration analysis determined which licenses you need? Firms operating without required money transmitter licenses or CFTC registration face immediate disqualification.
- If you trade futures or advise on commodity pools, provide CFTC/NFA registration documentation.
- Walk through your money transmitter analysis—which activities triggered review, which states require licensing, what analysis supported exemption claims?
- For international operations, provide all foreign registrations and explain jurisdictional analysis.

Compliance Program Independence

- How does the CCO maintain independence—reporting structure, budget authority, termination protections?
- Provide compliance testing reports from past 12 months showing methodologies, findings, and remediation.
- Walk through a recent compliance violation—how was it identified, investigated, remediated, and what controls were enhanced?
- What technology platforms support compliance monitoring for trading surveillance, personal trading, marketing review, and AML? How do you monitor regulatory developments?

AML Program and On-Chain Monitoring

- Walk through your KYC onboarding from initial contact through approval.
- What blockchain analytics tools monitor investor wallet activity post-onboarding?
- What specific triggers require enhanced due diligence?
- Describe the process from suspicious activity detection through SAR filing.

- How frequently do you screen against OFAC and sanctions databases?

Examination History

- Provide dates and scope of all regulatory examinations over past five years.
- Provide all deficiency letters received with full findings and response letters.
- For each deficiency, provide evidence of remediation implementation.
- What is your current examination status—any ongoing examinations or regulatory inquiries?
- Disclose all litigation, enforcement actions, or regulatory investigations.

Documentary Evidence Requirements

- Complete compliance manual with version control and board approval
- Compliance testing reports for past 12 months
- Training records with completion rates and attestations
- Violation logs with investigation documentation and remediation
- All examination correspondence including deficiency letters and responses
- Complete set of all registrations—federal, state, and international
- AML risk assessment and transaction monitoring reports
- SAR filing logs (redacted appropriately)
- Personal trading pre-clearance and exception logs

COMMON PITFALLS AND REMEDIATION

- *Registration analysis is incomplete or outdated*. Firm assumes SEC registration covers all activities, missing CFTC requirements for futures/swaps, state money transmitter triggers for custody operations, or foreign registration for non-US investors. Remediation: Obtain legal memorandum mapping each business activity to registration requirements. Review when adding strategies, investor types, or jurisdictions—and at minimum annually.
- *CCO lacks independence or crypto expertise*. CCO reports to CIO (compromising objectivity) or lacks blockchain knowledge to assess protocol risks, interpret on-chain activity, or evaluate custody controls. Remediation: Restructure reporting

to CEO or board with direct board access. Require CCO expertise in both traditional compliance frameworks and digital asset operations—or supplement with specialized external resources.

- *Compliance manual is a generic template*. Procedures reference "appropriate controls" without specifying what they are. Digital asset-specific risks—custody key management, DeFi protocol exposure, on-chain transaction monitoring—aren't addressed. Remediation: Customize every procedure to reflect actual operations. Add sections addressing wallet management, protocol due diligence, blockchain monitoring, and crypto-specific conflict scenarios.
- *No systematic compliance testing*. Policies exist but no one verifies they're followed. No testing schedule, no sample selection methodology, no documented findings. Remediation: Implement quarterly testing covering key controls—personal trading, best execution, valuation, custody procedures. Document methodology, samples tested, findings, and remediation actions in retained work papers.
- *Marketing materials bypass compliance review*. Pitch decks, performance presentations, and social media posts distributed without CCO approval—creating regulatory exposure from unsubstantiated claims or misleading performance. Remediation: Require documented CCO sign-off before any investor-facing material is distributed. Maintain archive of all materials with approval records. Train investor relations and business development on advertising rules.
- *Recordkeeping won't survive examination*. Documents scattered across email, personal drives, and multiple systems. No retention schedule, no consistent organization, no ability to produce complete records promptly. Remediation: Implement centralized repository organized by record type. Define retention periods by category. Test retrieval capability—if producing documentation for a single trade takes more than a few hours, the system needs improvement.
- *AML program ignores on-chain activity*. KYC collects standard documentation but doesn't screen wallet addresses, analyze transaction patterns, or monitor for sanctions exposure on-chain. Remediation: Implement blockchain analytics for investor wallet screening and ongoing transaction monitoring. Establish procedures for sanctions list screening of addresses and response protocols for identified risks.
- *Annual compliance review is a checkbox exercise*. Review document recites that "policies remain adequate" without analyzing testing results, violation trends, business changes, or control gaps. Remediation: Conduct substantive annual assessment covering: testing findings and remediation status, violations and root

causes, business or regulatory changes requiring policy updates, and specific improvement priorities. Present to board with implementation timelines.

KEY CONTROLS & DOCUMENTATION

Document	Purpose	Update Frequency	Owner
Compliance Manual	Comprehensive policies and procedures	Annual minimum	CCO
Code of Ethics	Ethical standards and personal trading rules	Annual	CCO
Form ADV	Registration and disclosure document	Annual + amendments	CCO
AML/KYC Policies	Customer due diligence and monitoring procedures	Annual	AML Officer
Marketing Policies	Advertising and communication standards	Semi-annual	CCO
Cybersecurity Policies	Data protection and incident response	Annual	CCO/CTO
Business Continuity Plan	Disaster recovery and operational resilience	Annual	COO
Regulatory Calendar	Filing deadlines and requirements	Monthly	Compliance
Training Records	Employee training and attestations	Ongoing	COO
Testing Documentation	Compliance testing results and remediation	Quarterly	COO
Violation Log	Compliance breaches and corrections	Ongoing	COO

Document	Purpose	Update Frequency	Owner
Examination Files	Regulatory correspondence and responses	As needed	COO

STANDARD 3: CONFLICTS OF INTEREST

Firms must identify and manage conflicts of interest. This includes systematic processes to identify all material conflicts affecting clients and the firm; code of ethics with personal trading policies, conduct standards, and enforcement mechanisms; and clear disclosure framework for material conflicts that cannot be avoided or mitigated. Firms must provide regular training and awareness programs for all personnel on conflicts identification and management and maintain monitoring and enforcement mechanisms with documented procedures for violations.

Conflicts of interest in digital asset management are inherent features of the ecosystem. The interconnected nature of blockchain technology creates conflicts not typically found in traditional finance. Examples include investment teams holding tokens personally while managing institutional portfolios, employees contributing to protocols in which the fund invests, service providers with multiple conflicting business lines, and the flow of material non-public information through both traditional channels and crypto-native platforms like Discord and Telegram. Generic conflict policies designed for traditional hedge funds often do not adequately address the complexities of digital assets.

Standard three emphasizes that firms should establish systematic frameworks to identify conflicts across all activities. These frameworks should manage conflicts through appropriate controls rather than relying solely on prohibitions. Transparency about material conflicts is essential to maintain fiduciary trust. This involves moving beyond generic policies to address specific challenges related to digital assets. Effective conflict management requires continuous monitoring, rather than annual reviews, enforcement that applies uniformly regardless of seniority, and transparent communication with clients about how conflicts are managed in practice, not just in policy.

Upholding this standard involves creating processes that naturally surface conflicts instead of hiding them. Management strategies should be calibrated to the severity of conflicts, with systematic documentation to demonstrate actual compliance. In some cases, conflicts are so severe that activities must be eliminated entirely to uphold fiduciary duties. Firms that attempt to maintain activities incompatible with fiduciary obligations risk creating conflicts that cannot be mitigated, which clients and institutional investors are unlikely to accept, regardless of mitigation efforts.

3.1 CONFLICT IDENTIFICATION & MANAGEMENT FRAMEWORK

An effective conflicts framework begins with clear understanding of the landscape. Digital asset managers face three primary conflict categories, each requiring sophisticated management approaches. Investment conflicts arise when different strategies or positions create competing interests—holding the same token in both venture and liquid portfolios creates allocation conflicts when new investment opportunities emerge. Personal conflicts emerge from individual activities within the crypto ecosystem—most professionals in this space hold tokens personally and participate in protocol governance. Structural conflicts embed themselves in the ecosystem's developing infrastructure—service providers often operate multiple conflicting business lines simultaneously.

Conflict identification requires systematic processes rather than relying on self-reporting alone. Quarterly attestations from all employees disclosing personal holdings, outside activities, and protocol involvement provide baseline documentation. On-chain monitoring using blockchain analytics verifies disclosed wallets and identifies undisclosed activity. Regular review of service provider relationships assesses whether counterparties' business evolution creates new conflicts. Investment committee procedures require disclosure of personal interests before position discussions. These systematic processes surface conflicts that individuals might rationalize as immaterial or overlook entirely.

3.1.1 THE CONFLICT RESPONSE STRATEGY

Once identified, conflicts require management strategies tailored to their nature and severity. The appropriate response depends on whether transparency alone provides sufficient protection, whether the conflict affects specific decisions requiring recusal, whether systematic separation prevents problematic interactions, or whether the conflict proves unmanageable requiring prohibition. Applying prohibition universally eliminates legitimate activities unnecessarily; applying disclosure alone to severe conflicts creates fiduciary breaches.

- *Disclosure:* Baseline response for manageable conflicts where transparency provides sufficient protection. Portfolio managers sitting on non-profit industry association boards create potential conflicts manageable through disclosure to investors and the board. Disclosure requires clarity—vague statements about 'industry involvement' prove insufficient. Specific activities, compensation, time commitments, and potential conflicts require explicit documentation in Form ADV and investor communications.
- *Recusal:* Effective strategy for managing conflicts affecting specific decisions. Investment committee members discussing protocols where they previously contributed should recuse from voting and exit during deliberations. Recusal

requires documentation—meeting minutes must record when individuals recuse and why. Patterns of frequent recusal signal that the underlying activity creates systematic conflicts requiring reassessment of whether the activity remains compatible with fiduciary obligations.

- *Separation:* For systematic conflicts, structural barriers prevent problematic interactions. Firms managing both venture and liquid strategies should implement information barriers preventing venture deal flow from reaching liquid portfolio managers before public announcement. Physical separation, separate reporting structures, restricted system access, and documented communication protocols create effective barriers. Barriers require enforcement—logs showing information sharing between separated teams reveal ineffective implementation.
- *Prohibition:* Reserved for unmanageable conflicts where activities cannot coexist with fiduciary duties. Trading against client interests, front-running fund trades, accepting undisclosed compensation from protocols the fund invests in, or using confidential fund information for personal benefit require absolute prohibition. Prohibition means termination for violations—enforcement inconsistency destroys policy credibility. Activities requiring prohibition but deemed strategically valuable create existential conflicts—firms cannot simultaneously maintain fiduciary standards and engage in conflicted activities.

TABLE 1: CONFLICT RESPONSE OVERVIEW

Strategy	When to Use	Implementation Requirements
Disclosure	Manageable conflicts where transparency provides sufficient protection	Specific disclosure in Form ADV, investor communications, and to board. Detail activity, compensation, time commitment, and potential conflicts.
Recusal	Conflicts affecting specific decisions but not systematic across activities	Document recusal in meeting minutes. Individual exits during deliberation and abstains from voting. Monitor frequency for systematic patterns.
Separation	Systematic conflicts requiring structural barriers to prevent problematic interactions	Physical separation, separate reporting, restricted system access, documented communication protocols. Audit logs verify barrier effectiveness.

Strategy	When to Use	Implementation Requirements
Prohibition	Unmanageable conflicts where activities cannot coexist with fiduciary duties	Absolute prohibition with termination for violations. No exceptions regardless of seniority. Document policy clearly with acknowledgment.

In conflict management, the core challenge is often not policy absence but incomplete identification of digital asset-specific conflicts. Traditional conflict frameworks may miss novel situations: protocol token holdings that benefit from fund activity, DeFi governance participation affecting holdings, validator relationships influencing execution, and equity stakes in service providers. Best practice is developing a digital asset-specific conflict inventory that supplements traditional categories. This should be reviewed periodically as the business evolves—new strategies, protocols, or service relationships may introduce conflicts not previously considered. Effective conflict management requires first acknowledging that conflicts exist; firms should document both identified conflicts and the controls applied to each.

3.2 PERSONAL TRADING & EMPLOYEE CONDUCT

Most professionals involved in digital assets hold tokens personally. Implementing policies that ban all personal investments could reduce the talent pool, as expertise in digital asset management often develops through personal participation in cryptocurrency markets and protocols. A better approach involves establishing systematic controls that allow appropriate personal investing while avoiding conflicts with fiduciary duties. Effective personal trading policies should include pre-clearance procedures, designated holding periods, blackout periods, and thorough monitoring. These measures help balance employee participation with investor protection, ensuring responsible management of personal investments in digital assets.

3.2.1 PRE-CLEARANCE AND MONITORING

Pre-clearance procedures establish essential controls requiring employees to obtain approval before engaging in personal trading activities. These controls are designed to protect the

integrity of the investment process while maintaining operational efficiency. Systems should require approval within defined timeframes to prevent front-running and avoid unnecessary delays that could interfere with legitimate personal investing activity. Investment managers operating in digital asset markets should implement these controls to ensure regulatory compliance and uphold fiduciary responsibilities. Clear and consistently applied pre-clearance processes promote transparency, accountability, and the overall integrity of the investment management framework.

The pre-clearance framework should include the following core requirements:

- *Universal coverage:* Require pre-clearance for all personal digital asset trades regardless of employee role, title, or seniority. Apply controls uniformly across the organization. Prohibit exemptions for senior management absent explicit board approval.
- *Holding periods:* Impose minimum holding requirements to discourage short-term speculative trading and reduce market-timing advantages. Require a minimum 30-day holding period for all employees. Apply extended holding periods (e.g., 90 days) for investment team members or employees with access to portfolio decision-making.
- *Restricted lists and blackout periods:* Prohibit trading in digital assets held by firm-managed funds, included on internal research or watch lists, or subject to pending fund transactions. Enforce blackout periods before and after anticipated fund activity to prevent front-running and information misuse.
- *DeFi activity disclosure:* Extend pre-clearance requirements beyond spot token transactions to include staking, liquidity provision, yield farming, protocol governance participation, airdrops, and NFT trading. Require heightened review and explicit approval for complex or multi-step DeFi interactions.
- *Timely processing:* Require Compliance to approve or deny standard pre-clearance requests within a defined timeframe (e.g., 24 hours). Maintain pre-clearance requirements during periods of heightened market volatility. Design procedures to accommodate the 24/7 nature of digital asset markets without weakening control standards.

Clear pre-clearance rules, combined with consistent enforcement and timely review, are essential to preventing conflicts of interest and preserving trust in the firm's investment and compliance framework.

On-Chain Monitoring Implementation:

Blockchain transparency allows for detailed monitoring that is not possible with traditional finance. Investment managers should use blockchain analytics tools to continuously observe

all employee wallets that are publicly disclosed. Monitoring systems should identify activities such as trades involving restricted tokens, transactions that occur before fund activity, links to undisclosed wallets, use of mixing services, and decentralized finance activities that have not been pre-approved. Monthly reconciliation processes compare on-chain activities with pre-clearance approvals to detect any unauthorized trading. This approach helps ensure compliance and enhances oversight in digital asset management, aligning with fiduciary standards and regulatory expectations.

3.2.2 ATTESTATION AND ENFORCEMENT

Effective monitoring requires supplementing automated surveillance systems with employee attestations and systematic testing. Attestations compel conscious acknowledgment of policy obligations and create formal documentary evidence of employee awareness, accountability, and compliance.

The attestation and enforcement framework should include the following components:

- *Quarterly certification:* Require all employees to certify on a quarterly basis that they have complied with the firm's personal trading policies. Confirm that all digital asset wallets and accounts have been fully disclosed. Attest that pre-clearance was obtained for all personal trades. Affirm that no undisclosed conflicts of interest exist.
- *Annual audit and testing:* Conduct an annual Compliance-led audit of personal trading activity. Sample employee trades to verify adherence to pre-clearance requirements, holding period rules, and restricted list prohibitions. Use both internal records and independent verification sources where appropriate.
- *New wallet disclosure:* Require employees to disclose newly created wallets or accounts within a defined timeframe (e.g., 10 days of creation). Treat failure to disclose wallets identified through on-chain analysis or forensic review as a policy violation.
- *Enforcement and escalation:* Apply violations consistently and proportionately based on severity. Issue written warnings for minor infractions (e.g., late pre-clearance submissions). Impose financial penalties for moderate violations (e.g., holding period breaches). Enforce termination or equivalent disciplinary action for serious violations, including trading restricted assets, maintaining undisclosed wallets, front-running, or misuse of material non-public information.

Consistent attestation, rigorous testing, and clearly defined enforcement consequences are essential to maintaining the credibility, deterrent effect, and regulatory defensibility of the firm's compliance framework.

Personal trading violations in digital assets often involve complex DeFi activities rather than simple token purchases. An employee might properly pre-clear a token acquisition but fail to disclose subsequently staking it, providing liquidity, or participating in governance—each creating distinct conflict implications that traditional pre-clearance systems may not capture. Best practice is extending monitoring beyond exchange accounts to include wallet addresses and on-chain activity. Employees should disclose all wallets, and compliance should have capability to monitor blockchain activity—either through internal tools or third-party blockchain analytics providers. Comprehensive monitoring demonstrates that policies are enforced consistently, not just documented.

3.3 OUTSIDE ACTIVITY MANAGEMENT

Professionals involved in digital assets actively engage in the wider industry by contributing to open-source projects, speaking at conferences, advising protocols, and participating in governance. These activities add valuable expertise and help establish industry presence. However, such involvement can lead to conflicts of interest that require careful management. Complete bans on outside activities could prevent beneficial industry engagement, while unmanaged participation might result in breaches of fiduciary duties. Effective management of outside activities involves implementing a process for prior approval, which includes evaluating potential conflicts, and ongoing monitoring as activities develop. This approach helps maintain integrity and compliance within the organization, supporting responsible participation in the digital asset ecosystem.

3.3.1 PRE-APPROVAL AND BOUNDARIES

All outside business activities must receive prior written approval from Compliance to identify, assess, and mitigate potential conflicts of interest. The review should evaluate both the current characteristics of the activity and the likelihood that the activity could evolve into a conflict over time.

The Compliance review should assess the following dimensions:

- *Nature of the activity:* Determine whether the activity is passive or active in nature. Distinguish between passive investments and active advisory, governance, or consulting roles. Evaluate open-source or community contributions versus compensated engagements. Differentiate educational

activities (e.g., conference speaking) from ongoing protocol or company involvement.

- *Time commitment and interference risk:* Evaluate the expected time commitment, including weekly hours and peak demands. Assess whether the activity could interfere with the individual's primary employment responsibilities. Consider whether outside obligations could conflict with firm priorities during periods of market stress or heightened workload.
- *Compensation and incentive alignment:* Review the form and structure of compensation, including cash payments, token grants, equity interests, or governance rights. Assess vesting schedules, lockups, and transfer restrictions. Evaluate whether compensation creates incentives that could conflict with the firm's investment positions or fiduciary obligations to clients.
- *Competitive and investment overlap:* Assess whether the activity competes with the firm's business, investment strategies, or client interests. Evaluate advisory or governance roles involving protocols, issuers, or companies in which the firm or its clients hold positions. Consider relationships with entities competing for similar investment opportunities.
- *Information access and confidentiality risk:* Evaluate whether the activity provides access to material non-public information or confidential data. Assess potential insider trading, misuse-of-information, or confidentiality risks. Review external confidentiality obligations for conflicts with the firm's fiduciary and compliance requirements.
- *Ongoing monitoring and re-approval:* Require annual re-approval and continuous oversight of approved activities. Reassess whether the scope, compensation, or influence of an activity has changed over time. Evaluate whether initially permissible activities—such as open-source protocol contributions—have evolved into compensated advisory roles or governance token grants that create misaligned incentives.

Clear boundaries and periodic reassessment are essential to prevent conflicts from developing incrementally and to ensure continued alignment with fiduciary responsibilities.

Related party failures typically occur when affiliate transactions lack arm's-length pricing validation or independent approval. Routing trades through affiliated venues, using affiliated administrators, or investing in affiliated protocol launches creates conflicts requiring specific controls beyond standard investment procedures.

Best practice is establishing a related party transaction policy requiring: identification of all affiliated entities, disclosure of any contemplated transaction, independent pricing validation, and approval by personnel not involved in the affiliated relationship (typically a committee or board). Documentation should capture the analysis supporting why the transaction serves client interests despite the affiliation.

3.4 INFORMATION BARRIERS AND CONFIDENTIALITY

Information is investment management's lifeblood and countless conflicts' source. In digital assets, information flows through both traditional channels and crypto-native platforms like Discord, Telegram, and governance forums. Material non-public information (MNPI) controls designed for traditional securities prove insufficient for digital asset complexity—protocol governance discussions, smart contract vulnerabilities, and validator network changes create MNPI absent from traditional finance.

3.4.1 DEFINING AND CONTROLLING MNPI

Digital asset MNPI includes traditional categories plus crypto-specific information. Material non-public information exists when: information is not publicly available, information would affect a reasonable investor's decision, and information was obtained through confidential relationships or sources. Digital asset-specific MNPI includes:

- Knowledge of upcoming protocol upgrades, forks, or major releases before public announcement
- Information about undisclosed security vulnerabilities in protocols or smart contracts
- Governance vote results before public disclosure or voting conclusion
- Major partnership announcements, token listings, or protocol integrations before public release

- Validator set changes, network hard forks, or consensus mechanism updates before implementation
- Material treasury transactions, token burns, or supply changes before execution

3.4.2 IMPLEMENTING INFORMATION BARRIERS

Effective information barriers require physical, technological, and procedural separation. Physical separation places teams in different locations or segregated areas. System access restrictions prevent information sharing through shared drives or communication platforms. Documented communication protocols establish when cross-barrier communication is permitted and how it must be documented.

- *Physical separation:* Different office locations, floors, or secured areas with access controls. Separate conference rooms and common areas.
- *System access:* Separate file servers, restricted document access, segregated email distribution lists. Monitoring logs showing access attempts and successful access.
- *Communication protocols:* Formal procedures for permitted cross-barrier communication. Legal or compliance approval required. Documentation of all barrier crossings with rationale.
- *Monitoring:* Regular audit of system access logs, email communication between separated teams, and physical access records. Testing barrier effectiveness annually.

3.5 VENDOR AND COUNTERPARTY CONFLICTS

Conflicts among service providers in digital assets are more common than in traditional finance because of ecosystem consolidation. Limited infrastructure means that the same entities often offer multiple services, such as exchanges running market-making operations, custodians providing prime brokerage, and data providers trading for their own accounts. These structural conflicts require thorough due diligence and continuous monitoring. Relying solely on contractual protections is insufficient; ongoing oversight is essential to manage potential conflicts effectively.

3.5.1 DUE DILIGENCE AND MITIGATION

A formal vendor conflict assessment must move beyond "check-the-box" exercises to analyze the following five pillars:

- *Business Line Overlap:* Identify whether a provider operates competing services, such as an exchange with an affiliated market maker or a custodian that also provides lending. The goal is to map where the provider's profit motives may diverge from the client's interests.
- *Information Access & Ethics:* It is critical to determine what sensitive client data the provider can access—specifically trading patterns, position data, or strategy details. The assessment must evaluate the risk of this information being leveraged by the provider's own proprietary trading desks or conflicting business units.
- *Incentive Structures:* Analyze the provider's compensation model to identify misaligned incentives. This includes evaluating the impact of payment for order flow (PFOF), lending fees, or trading profits that may encourage the provider to prioritize their own revenue over client execution quality.
- *Mitigation & Control Measures:* Verify the strength of the provider's internal safeguards. Fiduciaries should look for established Information Barriers ("Chinese Walls") between units, independent oversight of conflicted activities, and formal disclosure and consent procedures.
- *Alternatives Analysis:* Finally, the fiduciary must assess the broader market to determine if less-conflicted alternatives exist. This involves weighing the cost and operational impact of switching against whether the severity of a current conflict justifies a change in service provider.

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional allocators assess conflicts of interest by examining evidence of enforcement rather than relying solely on policy quality. They differentiate between firms where conflicts are identified systematically and those where conflicts are hidden until discovered externally. Firms claiming to have no conflicts may either lack effective monitoring or have cultures that discourage disclosure. When firms cannot provide specific examples of conflicts along with documented resolutions or cannot produce complete monitoring records, it indicates that conflicts management functions more as an aspiration than as an operational control.

Framework and Enforcement

- Walk through your conflict of interest policy from identification through resolution—what constitutes a conflict, who evaluates it, what management strategies are available, and how are decisions documented?

- Describe a recent conflict that was identified and managed—what triggered identification, how was it evaluated, what management approach was selected, and how is ongoing compliance monitored?
- Has any employee been disciplined for conflicts violations in the past two years? If yes, describe violation and disciplinary action. If no, explain detection methodology.
- How many conflicts were identified in the past year and what were the primary categories?

Personal Trading and Outside Activities

- How do you monitor personal trading including DeFi activities, staking, liquidity provision, and governance participation—not just centralized exchange transactions?
- What blockchain analytics tools verify employee compliance? Walk through your pre-clearance process—what requires pre-clearance, who approves, and what is typical turnaround time?
- What is your policy on outside business activities? Provide specific examples of activities approved and denied with rationale.
- How do you monitor approved outside activities on an ongoing basis?

Specific Conflict Management

- How do you handle venture versus liquid strategy conflicts when holding same token with asymmetric information?
- What happens when employees contribute to protocols the fund invests in?
- How do you manage service provider conflicts? Walk through a restricted list addition.

Culture and Enforcement

- What disciplinary actions were taken for violations? How do you train on conflicts?
- What anonymous reporting mechanisms exist? How does senior management model ethical behavior?

Documentary Evidence Requirements

- Complete Code of Ethics and conflicts policies
- Conflicts register (redacted) for past 12 months showing conflicts, management approach, and resolution

- Personal trading pre-clearance records (redacted) showing request volume and approval patterns
- Outside business activity log with approvals, denials, and ongoing monitoring
- Violation log with investigation summaries and disciplinary actions
- Training records and employee attestations

COMMON PITFALLS AND REMEDIATION

- *Policies enforced selectively by seniority*. Junior staff follow pre-clearance and disclosure requirements; senior personnel receive informal waivers or aren't questioned. Inconsistent enforcement destroys policy credibility and creates legal exposure. Remediation: Apply identical procedures regardless of seniority—same pre-clearance requirements, same documentation, same consequences for violations. Maintain logs demonstrating consistent enforcement across all levels.
- *Policies documented but not operational*. Well-crafted procedures exist in the compliance manual but don't reflect actual practice—no training conducted, no monitoring performed, no violations ever identified. Remediation: Test policy adherence through regular sampling and review. If testing never finds exceptions or issues, either the policy perfectly matches behavior (unlikely) or testing isn't rigorous enough.
- *Personal trading policy ignores DeFi activity*. Pre-clearance covers token purchases but not staking, liquidity provision, yield farming, or governance voting—each creating distinct conflict implications that traditional policies miss. Remediation: Expand personal trading coverage to all on-chain activity: staking, LP positions, protocol governance, airdrops, and wallet interactions with DeFi protocols. Require wallet disclosure and implement on-chain monitoring.
- *Information barriers cover email but not actual communication*. Formal systems are monitored while sensitive discussions happen on Telegram, Signal, Discord, or personal devices—rendering barriers ineffective. Remediation: Extend information barrier policies to all communication channels. Prohibit business discussion on unmonitored platforms. Train staff on what channels are permitted and consequences of circumvention.
- *Service provider conflicts unexamined*. Vendors selected for capability and cost without assessing whether their other relationships create conflicts—

administrator also serving competitors, custodian with affiliated trading desk, counsel representing adverse parties. Remediation: Include conflict assessment in vendor due diligence. Require disclosure of relationships that could compromise independence or create information leakage. Document assessment and any mitigating controls.

KEY CONTROLS & DOCUMENTATION

Document	Purpose	Frequency	Owner
Conflicts Policy	Main conflict framework	Annual	CCO
Code of Ethics	Ethics and trading rules	Annual	CCO
Conflict Register	Conflict tracking log	Monthly	Compliance
Personal Trading Records	Employee trading data	Quarterly	Compliance
G&E Log	Gifts and entertainment tracking	Ongoing	All Staff
Outside Activities	External activities log	Quarterly	Compliance
Restricted Lists	Trading restrictions	Daily	Compliance
Information Barriers	Access controls	Semi-annual	CCO
Vendor Conflicts	Provider conflict mapping	Quarterly	COO
Committee Minutes	Review decisions	Monthly	Secretary
Training Records	Training completion	Annual	CCO
Violation Log	Violations and remediation	Ongoing	CCO

STANDARD 4: INVESTMENT POLICY & GOVERNANCE

Firms must establish disciplined investment processes. This includes written investment policies aligned with stated objectives, strategies, and investor expectations; formal investment committee structure with documented decision-making processes and meeting cadence; and systematic performance measurement and attribution analysis appropriate to strategy. Firms must monitor investment guideline compliance regularly with escalation procedures for breaches and document clear procedures for strategy implementation and portfolio management activities.

Investment decisions in digital assets often happen under pressure. Market volatility demands quick responses, protocol updates require immediate assessment, and opportunities can disappear rapidly. This environment tempts managers to bypass disciplined processes in favor of quick, opportunistic actions. However, institutional capital benefits from systematic investment processes that operate independently of market conditions. Clear governance structures should constrain discretion, ensuring decisions follow established procedures rather than being justified after the fact.

Standard 4 emphasizes the importance of establishing disciplined investment processes. These processes should be supported by comprehensive investment policy statements that clearly define strategic boundaries. Investment committees should be structured to challenge proposals rather than approve them automatically. Research frameworks need to be applied consistently, regardless of how urgent the opportunity appears. All actions and decisions should be documented systematically to demonstrate that governance constraints are respected, especially during times of market stress. Flexible guidelines are acceptable only if they are part of a well-defined process that maintains discipline during volatile periods.

Creating effective governance involves developing documentation that governs decision-making rather than merely describing desired processes. Investment committees should actively challenge investment theses and record substantive deliberations. Research requirements should be applied uniformly, regardless of deal urgency. Rules for position sizing and portfolio construction should prevent excessive concentration. Sometimes, governance constraints may mean passing on attractive opportunities that do not align with the strategic plan. Maintaining flexible processes that justify any opportunity as strategic can undermine institutional standards, regardless of short-term performance outcomes.

4.1 INVESTMENT PHILOSOPHY & STRATEGY DOCUMENTATION

Clear and comprehensive investment documentation articulates the firm's core beliefs about markets, sources of potential returns, risk tolerances, and decision-making processes. Documentation serves three critical functions: constraining discretion through explicit boundaries, enabling due diligence through transparent disclosure, and facilitating performance attribution by establishing measurable objectives. Generic documentation stating the fund will 'invest in high-potential digital assets' provides no meaningful constraint on behavior and signals absence of genuine investment discipline.

4.1.1 INVESTMENT PHILOSOPHY

Your investment philosophy is your north star—the fundamental beliefs that drive every decision. Investors want you to explain *why* you invest the way you do—how markets work, where value accrues, and how those views translate into universe, sizing, exits, and limits. They're not just buying returns; they're buying a disciplined approach to producing them.

TABLE 1: CORE BELIEFS FRAMEWORK

Belief Category	Key Questions	Documentation Requirements	Review Frequency
Market Beliefs	How do digital asset markets function? What drives value?	Market structure thesis, efficiency assessment, adoption trajectory	Annual
Investment Beliefs	Where does alpha come from? What's our edge?	Alpha sources, risk-return framework, competitive advantage	Annual
Operational Beliefs	What infrastructure is essential? How do we engage?	Technology requirements, custody philosophy, governance approach	Semi-annual
Evolution Beliefs	How will the space develop? What changes expected?	Regulatory outlook, institutional adoption, technology roadmap	Quarterly

4.1.2 THE INVESTMENT POLICY STATEMENT (IPS)

The Investment Policy Statement (IPS) functions as the fund's operational constitution. It defines what the fund does, what it explicitly does not do, how decisions are made, and the constraints that govern behavior. Effective IPS documents provide sufficient specificity to

constrain discretion while maintaining the flexibility needed to execute strategy. To meet institutional standards, the IPS should comprehensively address:

- *Return Objectives and Time Horizon:* Target returns must be expressed numerically with clear time horizons. The policy should state whether returns are measured on an absolute basis or relative to benchmarks, and define expected volatility ranges. Vague objectives like "attractive risk-adjusted returns" should be avoided; specific targets enable meaningful performance assessment and investor alignment.
- *Risk Tolerances and Constraints:* Firms must establish specific numerical thresholds rather than aspirational statements about "appropriate risk management". This includes maximum drawdown limits with defined response procedures, volatility targets, and quantitative metrics like Value-at-Risk (VaR). The IPS must also specify liquidity requirements for redemptions and concentration limits to prevent excessive single-position exposure.
- *Investment Universe and Restrictions:* Explicit definitions of eligible asset types are required to prevent post-hoc rationalizations of inconsistent investments. Specific authorization is needed for Layer 1 protocols, DeFi tokens, NFTs, derivatives, staking, or venture investments. Prohibited investments—such as privacy coins or algorithmic stablecoins—must be clearly stated, along with any geographic or market-cap requirements.
- *Investment Process and Decision Authority:* The IPS must document how opportunities are sourced, screened, and researched before reaching the Investment Committee (IC). It should define IC composition, decision-making processes, and approval thresholds—clarifying which decisions require a full committee vote versus individual manager authority. Emergency procedures should be established for time-sensitive opportunities.
- *Portfolio Construction Framework*: Rules for building the portfolio must be specific enough for objective verification. This includes position-sizing methodologies based on conviction and liquidity, diversification requirements (such as minimum position counts or sector caps), and rebalancing triggers. The framework should also cover cash management and reserve requirements.
- *Risk Management Framework:* The policy must define the risk metrics to be calculated and their monitoring frequency. This includes a formal limit structure with escalation procedures for breaches, stress testing scenarios, and counterparty risk management—including exchange exposure limits and custody controls. Finally, it must specify who has the authority to override risk limits and under what circumstances.

4.1.3 STRATEGY-SPECIFIC DOCUMENTATION

Beyond the firm-wide IPS, each distinct investment strategy requires detailed documentation outlining its specific approach, unique risks, and operational procedures. Strategy-specific documentation enables specialized governance appropriate to each strategy's risk profile:

- *Venture Strategy Documentation:* Due diligence framework for evaluating early-stage projects including team assessment, technology review, tokenomics analysis, and competitive positioning. This must include valuation methodologies for illiquid tokens lacking market prices, investment thesis requirements, and monitoring procedures for portfolio companies. Additionally, it should cover follow-on investment criteria, exit strategy and liquidity timeline expectations, and governance rights negotiation and monitoring.
- *Liquid Strategy Documentation:* Identification of approved trading venues and their selection criteria. This requires a best execution policy with transaction cost analysis (TCA) procedures, order routing protocols, and market impact assessments for large positions. The documentation must also address counterparty risk management—including exchange exposure monitoring—and define the framework for high-frequency versus directional positioning and the weighting of technical versus fundamental analysis.
- *DeFi Strategy Documentation:* Protocol selection criteria emphasizing security audits, Total Value Locked (TVL) stability, and governance quality. It must establish a smart contract risk assessment framework and evaluate yield strategy sustainability. Furthermore, it should define impermanent loss calculations and acceptable ranges, protocol governance participation procedures, and emergency exit protocols for when protocol security is compromised.

> An investment policy provides value only when specific enough to constrain behavior. Generic language like "invest in digital assets consistent with fund objectives" offers no operational guidance. Effective policies establish specific parameters—eligible assets, concentration limits, leverage caps, liquidity requirements, and prohibited transactions—that create accountability and enable compliance monitoring. A practical test: review the IPS and identify a specific trade it would prohibit, then trace how that prohibition would be enforced before execution. If virtually any position could be rationalized as compliant, the policy may not be functioning as an effective control. Best practice is drafting policies specific enough that reasonable people could agree whether a proposed trade complies.

4.2 INVESTMENT COMMITTEE STRUCTURE & GOVERNANCE

The Investment Committee (IC) serves as the central decision-making body for all investment activities, providing forum for rigorous debate, challenging investment theses, and ensuring decisions align with strategy and risk tolerances. Effective Investment Committees distinguish themselves through substantive deliberation rather than perfunctory approval of pre-determined decisions. Committees that rubber-stamp CIO recommendations provide governance theater rather than meaningful oversight.

4.2.1 IC CHARTER AND COMPOSITION

The Investment Committee (IC) should operate under a formal charter that defines its mandate, authority, composition, and procedures. Charter specificity is critical for accountability; vague charters create confusion regarding decision authority and allow for post-hoc claims about whether a decision required IC oversight. To meet fiduciary standards, the charter must explicitly define:

- *Mandate and Authority:* Clear distinction between investment decisions requiring formal IC approval and those within individual portfolio manager discretion. Typical frameworks include thresholds where positions exceeding 5% of Net Asset Value (NAV) require IC approval, while smaller allocations remain within PM discretion. Additionally, adding any new asset class should always require IC authorization regardless of the position size.
- *Composition:* Identification of voting and non-voting members. Voting members typically include the Chief Investment Officer (CIO) as chair, senior portfolio managers, and heads of research. Non-voting members should include the Chief Risk Officer (CRO) for independent risk assessment and the Chief Compliance Officer (CCO) to ensure regulatory alignment. Participation by independent board members is recommended to further strengthen oversight.
- *Meeting Cadence*: A regular schedule with defined frequency appropriate for the strategy—such as weekly meetings for active liquid strategies and monthly sessions for venture strategies. The charter must also specify expedited procedures for ad hoc meetings to address time-sensitive investment opportunities.
- *Voting Procedures:* A clearly specified decision methodology, such as a simple majority vote, a supermajority for material positions, or unanimous consent for changes to the core strategy. This must include documented quorum requirements, rules for proxy voting, and formal procedures for recusal in the event of a conflict of interest.

- *Documentation Requirements:* Standardized protocols for meeting minutes, including templates, distribution procedures, and retention policies. Documentation must record the discussion summary, the rationale for each decision, any dissenting views, a tally of votes cast, and any disclosed conflicts.

4.2.2 IC MEETING PROCESS

Investment Committee meetings require structure enabling thorough evaluation while maintaining operational efficiency. Effective meetings balance adequate deliberation with timely decision-making—excessive bureaucracy causes missed opportunities while insufficient rigor enables poor decisions. The IC process should include:

- *Advance Agenda Distribution:* Circulation of a formal agenda at least 48 hours before meetings. This document should list all proposals requiring a decision, informational items, and necessary risk or performance reviews.
- *Pre-reading Materials:* Provision of comprehensive packages that include research reports, financial analysis, risk assessments, competitive analysis, and a recommendation summary. Materials must be detailed enough to allow members to evaluate the proposal independently.
- *Structured Presentation:* A formal briefing where the sponsor presents the investment thesis, key risks, valuation analysis, and position-sizing recommendations. Utilizing a standard template ensures consistent analysis across all opportunities.
- *Risk Officer Assessment:* An independent risk evaluation that covers potential portfolio impact, concentration implications, liquidity considerations, and limit compliance. This perspective must remain separate from sponsor advocacy to ensure objectivity.
- *Open Deliberation:* A structured debate designed to examine thesis assumptions, alternative scenarios, downside risks, and overall portfolio fit. Assigning a "devil's advocate" role can help ensure that contrarian perspectives surface during the discussion.
- *Documented Decision:* Formal minutes that record the discussion summary, the final decision, and the vote tally. Documentation must also include any dissenting views with their rationale, as well as specific conditions or monitoring requirements attached to the approval.

TABLE 2: INVESTMENT COMMITTEE CORE DELIVERABLES

Component	Requirements
Investment Memo	Comprehensive analysis covering: investment thesis, market opportunity, competitive analysis, team assessment, technology review, tokenomics evaluation, risk factors, valuation analysis, position sizing recommendation, exit strategy.
Risk Analysis	Independent assessment by risk function covering: portfolio impact analysis, concentration implications, correlation to existing positions, liquidity assessment, downside scenarios, stress test results, limit compliance verification.
Meeting Minutes	Formal documentation including: attendance, conflicts disclosed, summary of discussion, decision rationale, dissenting views, vote tally, conditions attached to approval, action items with owners.
Post-Investment Review	Periodic review of approved investments comparing actual performance to thesis, identifying thesis errors, documenting lessons learned. Conducted quarterly for large positions, annually for entire portfolio.

Investment committees add value through challenge and deliberation, not ratification. Committees that consistently approve all proposals without substantive discussion serve limited governance purpose—they provide a compliance checkbox without meaningful oversight. The value of committee governance is demonstrated through documented deliberation, questions raised, and instances where proposals were modified or enhanced. Best practice is including at least one independent or external member who brings perspective beyond the investment team, and maintaining minutes that capture substantive discussion—not just decisions. Periodic review of committee effectiveness (are proposals being improved through the process?) helps ensure the committee remains a genuine governance mechanism.

4.3 RESEARCH PROCESS & FRAMEWORK

Disciplined research processes are required to identify and evaluate investment opportunities systematically. Research frameworks must be structured, repeatable, and consistently applied, regardless of the source or urgency of an opportunity. Conducting opportunistic research under time pressure without a systematic framework leads to inconsistent analysis quality and enables confirmation bias, where analysts search for evidence to support pre-determined conclusions rather than performing an objective evaluation.

4.3.1 RESEARCH FRAMEWORK

Firms must maintain standardized frameworks for conducting research across all asset types to ensure consistent analysis of all material risk factors. Digital asset research frameworks should specifically address the following categories:

- *Technology Assessment:* A review of code quality, including security audit history, known vulnerabilities, and development activity. This must also include an evaluation of smart contract architecture, consensus mechanism analysis, and metrics regarding network security and decentralization.
- *Tokenomics Analysis:* An examination of supply schedules, inflation mechanics, and token distribution or unlock schedules. The framework should analyze utility and value accrual mechanisms, governance rights, voting power distribution, and the alignment of incentives between stakeholders.
- *Team Evaluation:* An assessment of founder backgrounds and track records, as well as the technical capabilities and relevant experience of the broader team. This includes reviewing advisory board quality, organizational structure, key person risks, and any history of project failures or successes.
- *Community Assessment:* Monitoring of active user metrics, growth trends, and developer contribution quality. Analysis should cover social media engagement, sentiment, governance participation rates, and the management of the community treasury.
- *Market Opportunity:* Determining the total addressable market size, competitive landscape, and key differentiators. The evaluation must also consider adoption trends, growth trajectories, sustainability of the business model, and jurisdictional or regulatory risks.
- *Valuation Analysis:* Application of comparable analysis methodologies and network value metrics such as NVT or NVU. When applicable, discounted cash

flow (DCF) models and scenario analysis (bull, base, and bear cases) should be used to derive price targets based on explicit assumptions.

4.3.2 RESEARCH DOCUMENTATION

All research must be recorded in formal reports and stored in centralized repositories. This documentation provides a historical record for post-mortem reviews, demonstrates a systematic process during due diligence, facilitates knowledge transfer during personnel changes, and serves as a baseline for monitoring investment theses. Research reports should include:

- *Executive Summary:* A concise overview of the investment thesis, key catalysts, major risks, valuation conclusion, and final recommendation. This should be detailed enough for Investment Committee members to understand the core arguments without reading the full report.
- *Detailed Analysis:* A comprehensive evaluation following the established research framework. All supporting data, calculations, and assumptions must be transparent and reproducible, with cited sources to enable verification.
- *Risk Assessment:* An explicit list of investment risks, including their probability and potential impact. This must cover downside scenarios, stress cases, mitigating factors, and specific metrics for ongoing monitoring.
- *Position Sizing:* A recommended position size expressed as a percentage of Net Asset Value (NAV), accompanied by a clear rationale. This should explain the relationship between conviction levels, liquidity, and sizing, including a build schedule if the position will be accumulated over time.
- *Monitoring Framework:* Identification of key metrics used to track the validity of the investment thesis. This includes "signposts" for thesis confirmation or invalidation and specific triggers for increasing, maintaining, or exiting the position.

Strategy drift occurs gradually—adding leverage, entering adjacent asset classes, increasing concentration—without formal acknowledgment or approval. Without defined limits and systematic monitoring, drift may go undetected until adverse performance materializes. The discipline of investment constraints protects both investors and managers by establishing clear boundaries for decision-making. Best practice is implementing hard limits with automated monitoring where possible, and clear escalation procedures when positions approach limits. Periodic review should assess whether any limits have never been approached—this may indicate either appropriate headroom or limits set so loosely they provide no practical constraint. Limits should occasionally bind; that's evidence they're calibrated appropriately.

4.4 PORTFOLIO CONSTRUCTION

Portfolio construction translates individual investment decisions into coherent portfolios aligned with strategy objectives and risk tolerances. Effective construction requires disciplined position sizing, diversification frameworks, and rebalancing procedures. Undisciplined construction enables excessive concentration in high-conviction positions, inadequate diversification across risk factors, and drift from the stated strategy as market movements alter portfolio composition.

4.4.1 POSITION SIZING AND DIVERSIFICATION

Position sizing methodology should balance conviction with diversification, liquidity with concentration, and upside potential with downside protection. Structured sizing frameworks prevent both excessive concentration, which creates catastrophic loss potential, and over-diversification, which eliminates alpha generation. Position sizing frameworks should address:

- *Maximum Position Size:* Hard limits expressed as a percentage of Net Asset Value (NAV). Typical ranges are 5–15% maximum per position depending on strategy and asset liquidity, with higher limits for large-cap liquid assets and lower limits for illiquid or venture positions.
- *Conviction-Based Sizing:* A framework relating position size to conviction level, thesis clarity, and the risk-reward profile. High conviction with asymmetric upside justifies larger positions, while uncertainty or a balanced risk-reward profile suggests smaller sizing.

- *Liquidity Considerations:* Position sizing should be inversely related to exit difficulty. Illiquid positions must be capped lower than liquid equivalents. Time-to-exit analysis should inform maximum size; positions requiring months to liquidate demand smaller allocations.
- *Diversification Requirements:* A minimum number of positions to prevent excessive concentration. This includes sector or category limits to prevent factor concentration and correlation analysis to ensure true diversification beyond simple position count.
- *Portfolio Impact Analysis:* Evaluation of new position sizing in the context of existing portfolio composition. This includes assessment of incremental risk contributions and stress testing the impact on overall portfolio metrics.

4.4.2 REBALANCING AND MONITORING

Portfolio composition drifts continuously through market movements, requiring systematic rebalancing procedures to maintain alignment with strategy and risk targets. Rebalancing frameworks should specify:

- *Rebalancing Triggers:* Thresholds that initiate rebalancing, such as a position exceeding its maximum size by a specified margin, a portfolio exceeding sector concentration limits, or risk metrics breaching defined targets.
- *Target Methodology:* Specification of whether rebalancing returns the portfolio to original weights, target weights, or defined acceptable ranges. The use of tolerance bands is recommended to prevent excessive trading costs.
- *Execution Procedures:* Documentation of who authorizes rebalancing trades, the execution timeline, and urgency assessments. This must include transaction cost analysis (TCA), acceptable price ranges, and market impact considerations for large rebalancing events.
- *Exception Procedures:* Conditions under which rebalancing may be delayed despite triggers, such as extreme volatility, liquidity crises, or thesis-driven concentration increases that require IC approval.

4.5 PERFORMANCE REVIEW & ATTRIBUTION

Comprehensive performance review and attribution analysis identify which investment decisions generate returns, whether results match thesis expectations, and what factors drive underperformance. This review process serves both accountability and learning functions—

tracking whether workflows generate expected results and identifying areas requiring improvement.

- *Attribution Analysis:* Decomposition of returns by position, sector, and strategy component. This involves identifying top contributors and detractors and comparing actual attribution to ex-ante expectations to reveal thesis accuracy.
- *Post-Investment Reviews:* A structured comparison of investment outcomes to the original thesis. This process identifies thesis elements proven correct or incorrect and documents lessons learned to improve future analysis.
- *Process Effectiveness:* Tracking decision quality independent of outcomes. Fiduciaries must assess whether the research methodology successfully identified key risks and evaluate the quality of IC deliberations and decision timeliness.

4.5.1 PERFORMANCE MEASUREMENT STANDARDS

Performance measurement requires frameworks that provide meaningful insights to institutional allocators. The chosen measurement approach must balance accuracy with practical limitations while demonstrating a sophisticated understanding of risk-adjusted returns. Allocators evaluate measurement quality as evidence of a firm's analytical depth and operational maturity.

While performance measurement in digital assets is challenged by extreme volatility, limited benchmarks, and an evolving market structure, institutional investors still expect rigorous analysis. This analysis must separate skill from general market movements, demonstrate a consistent methodology, and provide actionable insights for portfolio improvement.

TABLE 3: RETURN CALCULATION FRAMEWORK

Return Type	Methodology	Frequency	Key Adjustments
Time-Weighted	Geometric linking, flow adjusted	Daily	External flows, fee adjustments
Money-Weighted	IRR calculation	Monthly	Client experience focus
Risk-Adjusted	Sharpe, Sortino, Calmar ratios	Monthly	Downside risk emphasis
Benchmark-Relative	Excess return analysis	Monthly	Custom benchmark construction

Calculation Standards:

- Daily mark-to-market valuation using consistent pricing sources
- Proper treatment of cash flows and timing impacts
- Fee and expense allocation methodology
- Currency and operational cost adjustments
- Documentation of calculation methodology and data sources

> In the digital asset markets, there are no widely accepted benchmarks. It is important to document the process of how benchmarks are constructed clearly. Creating custom benchmarks that accurately reflect your specific investment universe is advisable, rather than relying on broad market indices that may not represent realistic investment opportunities. Clear documentation and tailored benchmarks help ensure transparency and relevance in performance measurement, supporting sound investment management practices in this evolving sector.

4.5.2 RISK-ADJUSTED PERFORMANCE METRICS

Digital asset performance measurement requires adapted metrics that account for extreme volatility, asymmetric return distributions, and unique market characteristics. Traditional risk metrics often fail to capture the true risk-return profile of digital assets, necessitating modified approaches that provide meaningful insights to institutional allocators.

Core Risk Metrics

- Modified Sharpe Ratio using downside deviation for asymmetric return distributions
- Sortino Ratio focusing on downside volatility rather than total volatility
- Maximum Drawdown including recovery periods and frequency analysis
- Calmar Ratio comparing annualized returns to maximum drawdown
- Value at Risk (VaR) across multiple confidence intervals and time horizons

Portfolio Risk Analysis

- Rolling volatility analysis across different time periods

- Correlation analysis with traditional asset classes
- Stress testing under multiple market scenarios
- Tail risk assessment and extreme event analysis
- Liquidity-adjusted risk metrics for illiquid positions

4.5.3 PERFORMANCE ATTRIBUTION FRAMEWORK

Performance attribution in digital assets requires decomposition of returns across multiple factors to identify skill versus market exposure. Digital asset attribution faces unique challenges including limited benchmarks, correlation instability, and crypto-specific risk factors that don't exist in traditional markets. Institutional allocators expect sophisticated attribution analysis that demonstrates active management value creation.

TABLE 4: ATTRIBUTION ANALYSIS (ILLUSTRATION)

Attribution Factor	Measurement Focus	Typical Impact	Analysis Frequency
Market Beta	Systematic market exposure	40-60% of variance	Daily monitoring
Security Selection	Alpha generation vs peers	20-30% of returns	Weekly analysis
Sector Allocation	Thematic positioning	10-20% of variance	Monthly review
Timing Decisions	Entry/exit execution	5-15% of returns	Monthly assessment
Operational Factors	Costs and efficiency	-2-5% of returns	Quarterly analysis

Attribution Analysis Requirements:

- Asset allocation decisions versus benchmark performance
- Security selection contribution across different market environments
- Timing effects from entry and exit decisions
- Cost analysis including transaction costs and management fees
- Risk-adjusted return analysis using appropriate benchmarks

4.5.4 REPORTING AND COMMUNICATION STANDARDS

Performance reporting should meet institutional standards for transparency, accuracy, and providing clear, actionable insights. It is important that reports are professionally presented to support evaluation and oversight by stakeholders. Investment managers in the digital asset space are expected to adhere to these guidelines to ensure accountability and maintain trust within the fiduciary framework. Clear and consistent reporting practices contribute to effective decision-making and uphold the integrity of the investment process, aligning with the expectations set by regulatory bodies such as the Securities and Exchange Commission (SEC) and industry standards established by the standard board for fiduciary investment management.

Monthly Performance Reports

- Executive summary with key performance highlights
- Detailed return analysis across multiple time periods
- Risk-adjusted performance metrics with peer comparisons
- Attribution analysis identifying return sources
- Portfolio statistics and position-level performance
- Market commentary and outlook discussion

Quarterly Comprehensive Analysis

- Detailed performance attribution across all factors
- Risk analysis including stress testing results
- Benchmark analysis and construction methodology
- Fee and expense analysis with transparency
- Strategy performance evaluation and lessons learned

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional allocators assess investment governance by examining their process discipline, decision documentation, and performance attribution. Demonstrating systematic research frameworks is essential. Investment committee minutes should reflect genuine debate, and explanations for position sizing decisions are necessary. These practices ensure the investment process is effective and transparent, aligning with fiduciary standards for digital asset management. Adherence to these principles supports sound decision-making and

accountability within investment organizations, fostering trust and integrity in the management of digital assets.

Investment Policy and Governance

- Walk through your Investment Policy Statement. How does it define investment universe, position limits, and risk tolerances?
- How is your Investment Committee structured and who are members? Provide redacted minutes from recent meeting showing discussion depth and decisions.
- Walk through a recent investment from idea to execution. What was your worst investment and what lessons were learned?
- Show examples of investments you rejected and why.

Research and Decision Process

- Show research report for your largest position demonstrating analysis depth.
- How do you handle fast-moving opportunities requiring rapid decisions?
- How do you generate alpha in crypto markets and what is your competitive advantage?
- How do you measure and improve process effectiveness?

Portfolio Construction

- What is your framework for position sizing and portfolio construction?
- How do you manage concentration risk?
- How do you think about correlation in crypto markets?
- Walk through your rebalancing process. How do you handle liquidity management?

Performance Measurement

- How do you measure and attribute performance? Explain your attribution methodology.
- What drives your returns and how do you benchmark performance?
- Walk through your worst drawdown. Can I see your most recent performance report?

Documentary Evidence Requirements

- Investment Policy Statement (IPS)
- Investment Committee charter and meeting minutes from past 6 months

- Sample investment memoranda and research reports
- Most recent investor letter and performance report
- Performance attribution reports
- Rebalancing documentation/ Strategy evolution documentation

---

COMMON PITFALLS & REMEDIATION

- *Vague IPS:* The Investment Policy Statement is overly broad, allowing nearly any investment to be rationalized as strategy-consistent. Remediation: Rewrite the IPS with specific numerical constraints, prohibited investment categories, and explicit approval thresholds. Test its robustness by reviewing recent exception approvals.
- *Rubber-Stamp IC:* The Investment Committee endorses CIO decisions without substantive debate or challenge. Remediation: Require independent risk assessments, document dissenting opinions, and assign a rotating devil's advocate. Track rejected proposals to evidence IC independence.
- *Inconsistent Research Application:* A research framework exists but is not applied uniformly across investments. Remediation: Audit the research repository to confirm full documentation for all positions. Deny IC consideration for incomplete submissions and track adherence to research protocols.
- *Undisciplined Position Sizing:* Position sizes are determined without a systematic framework, enabling excessive concentration. Remediation: Implement a clear sizing methodology linking position size to conviction, liquidity, and risk metrics. Record sizing rationale in IC minutes and monitor compliance daily.
- *Unmanaged Portfolio Drift:* Portfolio exposures deviate from target strategy due to market movements without systematic correction. Remediation: Deploy automated monitoring with defined rebalancing triggers and tolerance bands. Document all rebalancing actions and their rationale.
- *Absence of Post-Investment Review:* Investments are not evaluated against original theses, limiting organizational learning. Remediation: Conduct quarterly reviews for major positions and annual reviews for the full portfolio. Record thesis components validated or disproven, and capture insights for process refinement.

- Superficial IC Minutes: Meeting minutes are perfunctory, lacking substantive documentation of debate and rationale. Remediation: Expand the IC minutes template to capture key arguments, alternative views, risk factors, and decision justifications. Review minutes quality quarterly at the board level.

KEY CONTROLS & DOCUMENTATION

Document	Purpose	Frequency	Owner
Investment Policy Statement (IPS)	Investment guidelines and constraints	Annual	CIO/Board
Strategy Documentation	Strategy specifications and parameters	Semi-annual	CIO
Investment Committee Charter	Committee authority and procedures	Annual	CIO/Board
Research Methodology	Research framework and standards	Annual	Head of Research
Portfolio Construction Rules	Position sizing and allocation framework	Quarterly	CIO
Rebalancing Policy	Rebalancing triggers and procedures	Semi-annual	Portfolio Manager
Performance Methodology	Calculation and attribution methods	Annual	CFO
Investment Memos	Investment thesis and analysis	Per investment	Analyst/PM
IC Minutes	Committee decisions and deliberations	Per meeting	Secretary
Research Reports	Detailed investment research	Ongoing	Research Team
Attribution Reports	Performance decomposition	Monthly	Analyst/PM

Document	Purpose	Frequency	Owner
Position Limit Policy	Concentration and exposure limits	Quarterly	Risk/CIO
Trade Execution Policy	Best execution standards	Annual	Head of Trading
Benchmark Documentation	Performance comparison methodology	Annual	CIO/CFO

STANDARD 5: INVESTMENT OPERATIONS

Firms must maintain robust investment operations. This includes a best execution framework with regular assessment and documentation of execution quality; complete audit trail for all trading and investment activities with appropriate retention periods; and daily reconciliation processes with timely identification and resolution of breaks. Firms must maintain diversified trading relationships and venue connectivity appropriate to strategy and asset classes and establish operational controls appropriate for 24/7 market structure and digital asset characteristics.

Investment operations in digital assets are a critical part of risk management, not just back-office tasks. Transactions settle instantly and cannot be reversed, as there is no clearing house involved. Smart contracts, which automate transactions, can introduce coding errors that pose operational risks not found in traditional finance. Custody of digital assets requires understanding of private key cryptography, multi-signature schemes, and hardware security modules. Due to this operational complexity, firms need strong internal capabilities rather than relying solely on external fund administrators for managing digital assets.

Standard 5 highlights the need for a solid operational setup that meets the technical and operational needs of managing digital assets. This involves using advanced trading systems that can execute trades on multiple platforms and analyze transaction costs. Firms should also keep track of their positions across exchanges and custody providers in real-time. Additionally, they must create business continuity plans to handle specific failure scenarios related to digital assets. Operational failures can have serious consequences. For example, losing private keys permanently means losing access to assets; smart contract exploits can drain assets without recovery; and exchange hacks can cause losses that cannot be recovered from the counterparty.

Achieving this standard involves investing in scalable technology infrastructure and not underestimating operational requirements. It requires rigorous due diligence and testing of smart contracts, implementing multi-person authorization for significant transactions, maintaining comprehensive audit trails to demonstrate best execution and operational controls, and continuously investing in systems, personnel, and procedures. Managing institutional digital assets with inadequate operational infrastructure creates significant risks that investors will not accept, regardless of investment performance.

5.1 TRADING INFRASTRUCTURE AND TECHNOLOGY

Trading infrastructure functions as the technological backbone enabling investment execution. Infrastructure quality determines execution speed, multi-venue access, risk monitoring capability, and audit trail completeness. Inadequate infrastructure creates operational constraints limiting strategy execution, generates incomplete records complicating regulatory compliance, and introduces operational risks through manual processes and insufficient controls. Infrastructure requirements scale with strategy complexity—high-frequency strategies demand low-latency connectivity while venture strategies require robust position tracking and reporting systems.

5.1.1 SYSTEM ARCHITECTURE

Trading architecture combines proprietary systems, commercial platforms, and exchange connectivity into a cohesive operational infrastructure. Design priorities must emphasize reliability, security, scalability, and auditability over cost minimization. The core components of an institutional-grade system include:

Order Management System (OMS):

A centralized platform for managing orders, tracking positions, and monitoring risk in real-time. The OMS should aggregate positions across all venues and custody providers while calculating real-time P&L with mark-to-market pricing. It must enable order routing to multiple exchanges, maintain a complete audit trail of all trading activity, and integrate with compliance systems for trade surveillance.

Execution Management System (EMS):

Sophisticated execution tools that enable algorithmic trading, smart order routing, and transaction cost analysis. Core functionality includes Volume Weighted Average Price (VWAP) and Time Weighted Average Price (TWAP) algorithms to minimize market impact, limit order management across venues, and execution quality measurement through Transaction Cost Analysis (TCA). The EMS is essential for managing large positions that require careful execution.

Portfolio Management System (PMS):

The system responsible for maintaining the official books and records, including positions, transactions, cash movements, and performance calculations. The PMS should integrate with the OMS for trade capture, custody providers for reconciliation, pricing services for valuation, and fund administrators for NAV calculation. This component is critical for regulatory reporting, investor communications, and performance attribution.

Risk Management System:

A tool for real-time risk analytics that calculates exposure metrics, monitors limits, and generates alerts. The system should track position concentration, counterparty exposure, leverage utilization, VaR calculations, and stress test results. Direct integration with the OMS enables pre-trade risk checks to prevent limit breaches.

5.1.2 TECHNOLOGY GOVERNANCE

Formal technology governance processes are essential to ensure infrastructure reliability, security, and regulatory compliance. This framework provides oversight for vendor management, change control, cybersecurity, and disaster recovery:

- *Vendor Due Diligence:* A rigorous evaluation of third-party technology providers that includes security assessments, financial stability reviews, reference checks, and the negotiation of service level agreements (SLAs). Fiduciaries must also conduct annual vendor reviews to assess ongoing performance and continued suitability.
- *System Integration:* Documented integration plans for all new systems. These plans must cover data flows, API connections, testing procedures, and rollback protocols. Testing must be performed in non-production environments prior to any production deployment.
- *Change Management:* Formal control procedures for all technology updates. These requirements include written change requests with business justification, impact assessments for affected systems, and verification of testing before implementation. Rollback procedures and post-implementation reviews are mandatory to mitigate deployment risks.
- *Cybersecurity Program:* A comprehensive suite of security controls. This includes network segmentation, endpoint protection, intrusion detection, and vulnerability scanning. The program must also incorporate regular penetration testing, security awareness training for staff, and formal incident response procedures.
- *Access Controls:* Implementation of least-privilege access principles through role-based permissions. Multi-factor authentication (MFA) is required for all systems. Regular access reviews should be conducted to remove unnecessary privileges, and audit logging must track all administrative activities.

Best execution in fragmented crypto markets requires systematic analysis, not just competitive pricing. The same token may trade at materially different prices across venues at any given moment. Executing without documented consideration of available venues, their liquidity characteristics, and total execution cost may not satisfy best execution obligations. Best practice is maintaining an execution policy that specifies venue selection criteria, requires documentation of execution rationale for significant trades, and includes periodic transaction cost analysis. For large orders, pre-trade analysis of available liquidity across venues—considering depth, spread, and settlement characteristics—demonstrates the rigor institutional investors expect.

5.2 TRADE EXECUTION AND BEST EXECUTION

Best execution is the fiduciary duty to seek the most favorable terms for client transactions, considering factors such as price, speed, likelihood of execution, settlement certainty, and total transaction costs. In digital asset markets, which are often fragmented and less transparent than traditional securities markets, achieving and documenting best execution can be challenging. Multiple trading venues may offer the same asset but differ in liquidity, pricing, and counterparty risk. Therefore, systematic analysis of venues and careful selection of execution strategies are essential. Best execution involves both obtaining the best possible outcome and maintaining thorough documentation to demonstrate that the execution process systematically aims for optimal results rather than convenience. Investment managers should prioritize transparency and diligence in execution practices to uphold fiduciary responsibilities in the digital asset space.

5.2.1 BEST EXECUTION POLICY

A formal best execution policy outlines the internal processes for achieving and recording optimal transaction terms across all trading activity. The policy must comprehensively define the following:

Best Execution Factors:

Specific criteria used to evaluate execution quality, including quoted price, available liquidity, execution speed, and certainty. The policy must also account for market impact, information leakage, settlement risk, and counterparty credit quality. Factor weighting must vary by order characteristics; for instance, large orders prioritize minimizing market impact, while small orders emphasize price and speed.

Venue Selection and Monitoring:

A structured process for approving trading venues through due diligence. This assessment covers liquidity trends, pricing competitiveness, custody arrangements, and counterparty creditworthiness. It also includes a review of the venue's regulatory status, jurisdictional risks, and operational reliability. Ongoing monitoring must compare execution quality across venues to identify optimal options by asset and order size, supported by quarterly suitability reviews.

Transaction Cost Analysis (TCA):

A methodology for measuring execution costs systematically. The TCA framework should calculate implementation shortfall (comparing execution price to decision price), arrival price analysis for slippage, and VWAP comparisons for algorithmic trades. Additionally, it must include fee analysis across different venues and market impact assessments. Monthly TCA reports are required to identify performance trends and venue efficiency.

Documentation

Requirements: All material transactions require a clear audit trail demonstrating the pursuit of best execution. This includes the order rationale, urgency assessment, venue selection justification, and the reasoning behind the chosen execution strategy. Documentation must also incorporate post-trade TCA analysis and lessons learned. These records prove regulatory compliance and demonstrate execution discipline to institutional allocators.

5.2.2 EXECUTION STRATEGIES

Different execution strategies are available to optimize trading based on factors such as order size, urgency, and current market conditions. When choosing a strategy, it is important to consider the characteristics of the trade and the specific objectives of the execution. Investment managers in the digital asset space should evaluate these elements carefully to ensure effective and compliant trading practices. Adopting a well-informed approach to strategy selection supports fiduciary responsibilities and aligns with best practices outlined by the SEC and other regulatory bodies. Consistent application of these principles helps maintain market integrity and promotes efficient asset management:

- *Algorithmic trading:* Algorithms break large orders into smaller pieces executing over time minimizing market impact. VWAP algorithms target volume-weighted average price, TWAP algorithms spread execution evenly over time, implementation shortfall algorithms balance speed versus impact. Algorithmic execution requires EMS connectivity and venue access supporting programmatic trading.
- *Direct market access (DMA):* Executing trades directly on exchange order books provides price transparency and control. Appropriate for standard-size orders in

liquid markets where posted liquidity sufficient. Requires order management systems with exchange connectivity and real-time market data.

- *Over-the-counter execution (OTC):* Trading directly with market makers for large or illiquid positions prevents market impact and information leakage. OTC execution requires: multiple market maker relationships for competitive quotes, reference pricing from exchange data verifying reasonableness, documentation of quote solicitation and selection, credit assessment of OTC counterparties.
- *Smart order routing (SOR):* Automated routing to venues offering best prices and liquidity. SOR systems monitor multiple venues simultaneously, route orders dynamically based on real-time conditions, and aggregate partial fills across venues. Essential for firms trading across numerous exchanges.

Reconciliation delays compound quickly. A break unresolved for days can mask errors, fraud, or custody issues that grow harder to untangle over time. Daily reconciliation of all positions to independent sources (custodian statements, exchange records, blockchain data) is the operational baseline for institutional-quality operations. Best practice is establishing break aging thresholds with escalation requirements—for example, any break unresolved after three business days requires escalation to senior operations and documentation of resolution efforts. Regular reporting on reconciliation status, including break aging and resolution trends, demonstrates operational discipline to allocators and auditors alike.

5.3 DIGITAL ASSET OPERATIONS

Digital asset operations involve specific processes and controls that are different from traditional asset management. These include managing digital wallets, interacting with smart contracts, authorizing on-chain transactions, and participating in decentralized finance protocols. Such operations require a clear understanding of blockchain technology, cryptographic security, and how smart contracts work. Errors in handling digital assets are often irreversible. Transactions cannot be recalled, smart contract interactions cannot be undone, and assets sent to incorrect addresses are permanently lost. Investment managers should be aware of these risks and ensure proper procedures are followed to minimize errors and protect assets effectively.

5.3.1 WALLET MANAGEMENT

Formal wallet management policies establish essential controls to prevent operational errors and security breaches. Wallet operations must utilize multi-layered security and rigorous authorization procedures:

- *Multi-signature Architecture:* All material wallets should require multiple signatures to authorize transactions. Typical configurations include 2-of-3 for operational wallets, 3-of-5 for treasury wallets, and 4-of-7 for cold storage. Signers must be distributed across different individuals and geographic locations to eliminate single points of failure.
- *Hardware Security Modules (HSMs):* Private keys should be stored in HSMs or hardware wallets that are never exposed to network-connected systems. Key generation must occur within this secure hardware, and backup procedures must ensure key recovery can occur without compromising security.
- *Address Whitelisting:* All external addresses must be whitelisted before they can receive transactions. The whitelisting process requires address ownership verification (via signed message or test transaction), a documented business justification, dual approval from separate individuals, and a mandatory waiting period before activation. This prevents assets from being sent to incorrect or malicious addresses.
- *Transaction Authorization:* Multi-person approval is required for all outbound transactions. The process includes initiation with business justification, independent verification of the amount and destination, dry-run testing on a testnet when possible, final approval from authorized personnel, and post-transaction confirmation of settlement.
- *Wallet Inventory:* A complete registry must be maintained of all wallets, including addresses, custody arrangements, authorized signers, asset types, and purpose. Regular reconciliation is required between the inventory and actual holdings, and abandoned wallets must be identified so assets can be recovered or disposed of properly.

5.3.2 SMART CONTRACT INTERACTION

Interacting with DeFi protocols and smart contracts introduces operational risks that require formal approval and testing. Every interaction should be treated as a material operational decision subject to rigorous due diligence:

- *Smart Contract Due Diligence:* A thorough assessment must be conducted before approving protocol usage. This includes reviewing audit reports from reputable firms, internal or external code reviews, historical incident analysis, and

assessments of Total Value Locked (TVL) and usage patterns. It also requires evaluating governance and upgrade mechanisms, as well as insurance availability and coverage terms.

- *Transaction Simulation:* All contract interactions must be simulated in test environments before execution on the mainnet. Simulation verifies that expected state changes occur correctly, gas costs remain acceptable, no unexpected permissions are granted, and slippage/price impact stay within tolerances. Tools such as Tenderly or Phalcon should be utilized for this purpose.
- *Authorization Procedures:* Smart contract interactions require an approval hierarchy based on materiality. While small routine transactions may proceed with a single approval, novel protocol interactions require Investment Committee authorization. Documentation must include the protocol description, the function called, business rationale, risk assessments for worst-case scenarios, and simulation verification.
- *Emergency Procedures:* Response plans must be established for exploits or emergencies, including monitoring systems to detect unusual activity and emergency contact protocols for protocol teams. Designated personnel must have the authority to exit positions immediately without standard approvals, supported by communication protocols for stakeholders and post-incident lessons-learned documentation.

Digital asset corporate actions—airdrops, forks, staking rewards, governance distributions—require procedures that don't exist in traditional markets. Missing a fork deadline or failing to claim an airdrop directly reduces client value, and unlike traditional securities, there's no central depository ensuring proper receipt and allocation. Best practice is maintaining a protocol event monitoring process that tracks upcoming events across held assets, documents decisions made (participate or not, and rationale), and ensures proper allocation of any proceeds across client accounts. Firms should be able to demonstrate how a recent protocol event was identified, evaluated, decided, and allocated.

5.4 MULTI-CHAIN AND DEFI OPERATIONS

Operating across multiple blockchains and DeFi protocols requires sophisticated understanding of each network's unique characteristics while maintaining standardized

processes ensuring consistency and control. Multi-chain operations introduce complexities around gas mechanics, finality assumptions, and protocol-specific risks that demand systematic operational frameworks.

5.4.1 MULTI-CHAIN OPERATIONAL REQUIREMENTS

Each blockchain presents distinct operational requirements demanding tailored procedures:

- *Ethereum Operations:* Complex gas mechanics require sophisticated optimization strategies. The EIP-1559 base fee plus priority fee structure demands dynamic fee management, as high gas prices during network congestion can make transactions uneconomical. MEV protection is essential to prevent sandwich attacks and front-running. Transaction nonce management is critical for sequential processing, and monitoring the mempool is necessary for transaction status and identifying potential stuck transactions.
- *Bitcoin Operations:* The UTXO model requires different accounting approaches than account-based chains. Fee estimation is challenging during high network activity. Confirmation requirements typically mandate a 6-block minimum for material amounts. RBF (Replace-By-Fee) procedures are necessary for stuck transactions. Address type considerations (Legacy, SegWit, Taproot) affect both fees and compatibility.
- *Alternative Layer 1 Blockchains:* Each chain has unique consensus mechanisms affecting finality assumptions. Solana requires managing priority fees and understanding network congestion patterns. Avalanche subnets introduce additional complexity around cross-subnet operations. Network-specific risks include validator centralization and governance structures.
- *Layer 2 Solutions:* Bridging operations introduce additional complexity and risk. Withdrawal delays vary significantly across L2 solutions—for example, 7 days for Optimistic Rollups versus faster ZK-Rollups. Bridge security becomes a critical operational consideration. Gas optimization differs between L1 and L2, and monitoring L2 sequencer health and potential downtime is required.

5.4.2 DEFI PROTOCOL OPERATIONS

DeFi protocol interactions require a systematic framework from initial due diligence through ongoing position management:

- *Phase 1: Protocol Due Diligence:* Comprehensive assessment before any protocol interaction. This includes smart contract audit reviews from multiple reputable firms (minimum two independent audits), code reviews by internal developers or external specialists, team assessments, and sustainability analysis of the economic model. It also requires analyzing TVL trends, user adoption patterns,

governance structures, upgrade procedures, historical incident analysis, and insurance availability.

- *Phase 2: Position Entry:* A graduated approach to new protocol exposure. This includes a test transaction with a minimal amount to verify functionality, gradual scaling over multiple transactions to monitor for issues, and position size limits during the initial period (e.g., maximum 5% of protocol allocation in the first 30 days). Interactions must be documented with rationale and approvals.
- *Phase 3: Ongoing Management:* Continuous monitoring and active management of DeFi positions. This involves yield collection procedures, rebalancing triggers responding to rate changes, governance participation decisions, and impact assessments for protocol upgrades. It also requires tracking collateralization ratios for lending, monitoring impermanent loss for liquidity provision, and monitoring position size against protocol risk limits.
- *Phase 4: Exit Planning:* A systematic approach to position unwinding. This includes liquidity assessment for exit sizing, market impact analysis for large positions, gas cost optimization for exit transactions, and slippage tolerance parameters. Emergency exit procedures must be ready if protocol compromise is suspected, with documentation of exit rationale and execution.

DeFi Risk Management Requirements:

- *Position Size:* Maximum position size per protocol, typically 10–15% of protocol allocation.
- *Audit Standards:* Minimum of two independent audits from recognized firms.
- *TVL Thresholds:* Minimum TVL (e.g., $100M+) before material exposure.
- *Governance:* Active monitoring for parameter changes.
- *Emergency Controls:* Established emergency exit authority and procedures.

5.4.3 STAKING OPERATIONS

Staking operations require balancing yield optimization with liquidity management and operational risk:

- *Validator Selection Framework:* Comprehensive criteria for validator selection including performance history, uptime statistics, commission rates, fee structures, infrastructure quality, and geographic distribution. Assessment also includes slashing history, risk management, governance behavior, minimum self-stake ("skin in the game"), and responsiveness.

- *Liquidity Management:* Critical consideration of unbonding period constraints. These vary by chain (e.g., Ethereum: ~1 day; Cosmos: 21 days; Polkadot: 28 days). Fiduciaries must maintain unstaked reserves for liquidity, evaluate liquid staking derivatives (stETH, rETH) and their associated risks, and model worst-case liquidity scenarios accounting for unbonding delays.
- *Reward Management:* A structured approach to staking rewards, including claiming frequency optimization (gas costs vs. compounding benefits), auto-compounding vs. manual reinvestment, tax implications of timing, and separate accounting for rewards.
- *Staking Risk Monitoring:* Ongoing oversight of staking-related risks, including validator performance/downtime, slashing events and risk triggers, network-wide slashing incidents, and governance proposals affecting parameters. It also includes monitoring protocol upgrades and changes in validator commissions.

How errors are handled reveals operational culture. Every error—regardless of size—should be documented, investigated for root cause, and reviewed for process improvements. The goal is not zero errors (unrealistic in any operation) but systematic learning that reduces error frequency and impact over time. Best practice is maintaining an error log that captures: what happened, how it was discovered, root cause analysis, client impact and resolution, and process changes implemented. Periodic review of error patterns can identify systemic issues requiring broader remediation. A mature operations function acknowledges errors occur and demonstrates systematic improvement.

5.5 OPERATIONAL SECURITY FRAMEWORK

Operational security involves implementing comprehensive controls to address both traditional cybersecurity threats and vulnerabilities specific to cryptocurrencies. The irreversible nature of blockchain transactions and the continuous operation of markets present unique security challenges. A single compromised credential can lead to immediate and unrecoverable financial losses. Investment managers in the digital asset space should prioritize robust security measures to safeguard assets and maintain trust. It is essential to understand the risks associated with blockchain technology and to establish protocols that mitigate potential threats effectively. Regular security assessments, strong authentication practices, and

continuous monitoring are key components of a sound operational security strategy in this domain.

5.5.1 AUTHENTICATION AND ACCESS CONTROLS

Multi-factor authentication serves as foundational security control for all systems handling digital assets. However, not all MFA implementations provide equivalent security—SMS-based two-factor authentication remains vulnerable to SIM-swapping attacks that have cost crypto firms millions in losses, while hardware-based authentication provides substantially stronger protection against credential compromise. The authentication framework must distinguish between system types based on risk profile, applying strongest controls to systems with direct financial access while maintaining operational efficiency for lower-risk systems.

TABLE 1: AUTHENTICATION REQUIREMENTS BY SYSTEM TYPE

System Type	Minimum Standard	Recommended Practice	Prohibited Methods
Exchange Accounts	Hardware 2FA + IP whitelist	Hardware key + withdrawal address whitelist	SMS 2FA, email-only
Custodian Access	Hardware key required	Multiple hardware keys, time delays	Software 2FA alone
Internal Trading Systems	MFA mandatory	Hardware key + biometric	Password-only
API Access	API key + IP whitelist	Encrypted keys + rotation schedule	Plain text storage

Hardware security keys (YubiKey, Google Titan, or similar FIDO2-compliant devices) provide the strongest authentication protection and should be mandatory for all systems with direct financial access. These physical devices prove resistant to phishing, man-in-the-middle attacks, and credential theft that compromise software-based authentication methods. Organizations should deploy keys from multiple manufacturers avoiding single-vendor dependency and maintain backup keys in secure storage for emergency access.

API Key Management & Least Privilege:

Specialized protection for exchange API keys given potential for immediate financial loss: never store keys in plain text, implement HSMs or dedicated key management services for production keys, encrypt all keys at rest using AES-256, store encryption keys separately from encrypted data, mandatory quarterly key rotation, immediate rotation following personnel changes or security incidents.

To mitigate the risk of immediate financial loss, exchange API keys must be governed by the principle of least privilege. Many exchange compromises stem from overly permissive keys that allow unauthorized withdrawals despite being intended solely for trading.

Fiduciaries must implement the following granular permission standards:

- *Withdrawal Separation:* Trading keys must never possess withdrawal capabilities. Permissions should be restricted so that even if a trading key is leaked, assets cannot be moved off the platform.
- *Functional Segregation:* Maintain distinct keys for specific tasks, such as read-only monitoring (for portfolio tracking), trading operations, and withdrawal functions.
- *IP Whitelisting:* Restrict API access exclusively to known, trusted infrastructure. This ensures that even if a key is stolen, it remains useless when accessed from an unauthorized location.
- *Time-Based Restrictions:* For non-critical functions, limit API functionality to standard operational hours to reduce the window of vulnerability.

Continuous Oversight & Auditing

Static API keys represent "ticking time bombs" if left unmanaged. Effective oversight requires:

- *Quarterly Reviews:* Conduct formal audits to verify that every active key's permissions still match current operational requirements. Any keys identified as excessive or unused must be revoked immediately.
- *Automated Monitoring:* Deploy systems to track API usage patterns in real-time. Monitoring should automatically flag anomalies, such as unexpected spikes in traffic or access attempts from unrecognized IP addresses, for immediate forensic investigation.
- *Key Rotation:* Implement a mandatory rotation schedule (typically every 30–90 days) to limit the lifetime of any single credential.

Role-Based Access Control (RBAC):

Align permissions with job responsibilities and ensure segregation of duties. This approach helps maintain proper control and accountability within the organization. Investment managers in the digital asset space are advised to assign access rights based on specific roles and responsibilities. Clear separation of duties reduces the risk of conflicts of interest and enhances operational integrity. It is important to regularly review permissions to confirm they remain appropriate and aligned with current responsibilities.

TABLE 2: RBAC MATRIX

Role	Trading Access	Withdrawal Rights	System Administration
Portfolio Manager	Full trading	Initiate only	None
Operations Manager	View only	Approve only	Operational systems
Risk Manager	Read-only	Veto power	Risk systems only
Developer	None	None	Development environment only

Regular access reviews help ensure permissions stay aligned with current job roles as responsibilities change. Conducting quarterly audits verifies that each user's access matches their current position, and unnecessary permissions are revoked promptly. When employees leave the organization, their access should be terminated immediately to prevent unauthorized entry. Audit logs are important for tracking all access to financial systems, with automated alerts for unusual activities such as access from unexpected locations or outside normal working hours.

5.5.2 WITHDRAWAL CONTROLS

Withdrawal controls represent the critical last line of defense preventing unauthorized asset transfers. The irreversibility of blockchain transactions means that once assets leave firm control, recovery is effectively impossible. Tiered approval requirements based on withdrawal amount ensure oversight proportional to financial materiality—small operational withdrawals proceed efficiently while large transfers receive executive and board scrutiny. Time delays between approval and execution provide an additional window for detecting fraudulent requests before finality.

TABLE 3: TIERED APPROVAL REQUIREMENTS BY AMOUNT

Amount	Approval Required	Time Delay	Additional Controls
<$100,000	Single approval	None	Whitelisted addresses only
$100,000 - $1M	Dual approval	4 hours	Email confirmation
$1M - $10M	C-level approval	24 hours	Investment committee notification
>$10M	CEO + Board	48 hours	Board resolution required

The approval hierarchy should escalate automatically based on the withdrawal amount, with clear documentation requirements at each tier. Email confirmations provide out-of-band verification that approvers consciously authorized transactions. Investment committee notification for large withdrawals enables collective oversight to detect unusual patterns. Board-level approval for the largest withdrawals ensures the highest level of organizational awareness for material asset movements.

Address Whitelisting Requirements:

Protection against address substitution attacks is essential to maintain control over funds.

- *Seasoning Period:* New addresses should undergo a "seasoning" period of 48 to 72 hours before being used in production.
- *Test Transactions:* Small test transactions are recommended to verify control over new addresses prior to executing large transfers.
- *Multi-Party Verification:* Quorum-based verification processes should confirm address accuracy through independent communication channels.
- *Regular Reviews:* Quarterly reviews are advised to remove unused addresses and ensure only verified destinations remain active.
- *Compliance Documentation:* Documenting each address's purpose and authorization is necessary to maintain security and regulatory alignment.

Withdrawal Process Controls:

Procedures for withdrawals must be systematic and follow a strictly defined workflow:

1. *Initiation:* Authorized personnel initiate withdrawals with a documented, valid business reason.
2. *Independent Verification:* The destination address is independently verified to prevent errors or fraudulent substitution.
3. *Amount Verification:* The specific transaction amount is checked by a different person to ensure accuracy.
4. *Simulation:* For new destinations, a test transaction or simulation is required before the material withdrawal occurs.
5. *Final Approval:* Final sign-off is given only after the designated time delay for that tier has passed.
6. *Settlement Confirmation:* After the transaction, confirmation of successful on-chain settlement must be obtained and documented in the audit trail.

5.5.3 KEY MANAGEMENT HIERARCHY

Managing private keys is the most vital component of securing digital assets. Unlike traditional finance, where credentials can be revoked and fraudulent transactions reversed, compromised private keys lead to the instant and permanent loss of assets with no possibility of recovery.

A rigorous hierarchy for key management is essential to balance security requirements against the operational efficiency needed for daily activities. Fiduciaries should adopt a tiered storage framework that allocates the vast majority of assets to highly secure offline environments while maintaining smaller portions in more accessible tiers for active trading.

TABLE 4: STORAGE TIER FRAMEWORK

Storage Tier	Use Case	Security Requirements	Access Protocol
Cold Storage	Long-term holdings (>80% of assets)	Multi-signature (3-of-5 or 4-of-7), geographic distribution, bank vault storage	Multiple approvals, board notification, 48-72 hour delay
Warm Storage	Operational reserves (10-	Multi-signature (2-of-3), institutional custody, segregated	Dual approval, same-day access

Storage Tier	Use Case	Security Requirements	Access Protocol
	15% of assets)		
Hot Wallets	Daily operations (<5% of assets)	Single signature with transaction limits, HSM-secured	Single approval, real-time monitoring
Exchange Accounts	Active trading (5-10% of assets)	API keys, withdrawal address whitelist	System limits, automated alerts

Storage Rebalancing & Governance

Asset allocation across storage tiers requires a formal review at least monthly. Rebalancing becomes mandatory when actual allocations significantly deviate from policy targets.

- *Inbound Transfers:* Market volatility can cause exchange account balances to exceed set thresholds, requiring immediate transfers to cold storage to mitigate counterparty risk.
- *Outbound Transfers:* Active trading strategies may demand transferring assets from cold storage to warm storage to maintain necessary operational liquidity.
- *Documentation:* Every transfer between storage tiers must be documented with a clear business justification and approved through the appropriate tiered hierarchy. Routine rebalancing follows standard operating procedures, whereas urgent transfers require high-level approval from senior management or executives.

Key Management Lifecycle

Fiduciaries must maintain comprehensive procedures covering the entire journey of a cryptographic key:

- *Generation:* Keys must be generated within secure, tamper-resistant hardware (HSMs or hardware wallets) using true random number generators.

- *Storage & Backup:* Secure backup procedures must utilize geographic distribution to prevent local disasters from causing total loss.
- *Rotation & Revocation:* Mandatory rotation schedules minimize the risk of long-term compromise. Procedures must also ensure immediate revocation of access upon personnel changes.
- *Succession:* Clear planning ensures continuity if a primary key holder becomes unavailable.

Key Recovery Testing

Recovery procedures must be validated regularly through proactive testing rather than waiting for a crisis:

- *Drills:* Conduct quarterly recovery drills with rotating responsibilities to ensure staff competency.
- *Scenarios:* Testing should include diverse failure modes, such as key holder unavailability, physical hardware failure, and geographic disruption.
- *Refinement:* Documentation of lessons learned from drills should directly inform updates to the primary recovery procedures.
- *Verification:* Drills must verify that asset recovery is possible within the timeframes defined by the firm's Business Continuity Plan (BCP).

5.5.4 INCIDENT RESPONSE REQUIREMENTS

Security incidents require quick action because digital assets can be lost or damaged very fast. Traditional response times, which take hours or days, are too slow since attackers can drain wallets in minutes. The incident response plan should clearly define who has the authority to make decisions so actions can be taken immediately without delays.

It is also important to have procedures in place for common types of incidents, allowing for fast response even when stress levels are high. These procedures should include steps for escalating issues to senior management and the board of directors when necessary. Having a well-prepared plan helps ensure that responses are effective and timely, protecting digital assets and maintaining trust in the management process.

TABLE 5: INCIDENT RESPONSE BY TYPE

Incident Type	Response Time	Initial Actions	Escalation
Compromised Credentials	Immediate	Reset passwords, rotate API keys, review logs, notify counterparties	Security team + CTO
Suspicious Transaction	Immediate	Suspend trading if appropriate, monitor blockchain, engage law enforcement if material	CEO + Board
Exchange Security Alert	15 minutes	Verify alert validity, assess exposure, prepare withdrawal if necessary	Risk + Operations
Protocol Exploit	Immediate	Exit positions if possible, assess exposure, communicate with protocol team	Investment + Risk teams

Response time requirements are set based on the urgency of each incident type and its potential financial impact. Immediate response involves taking action within minutes, with systems ready to execute predefined procedures without waiting for management approval when seconds are critical. A fifteen-minute response window allows for a brief assessment before taking action, suitable when the threat is less immediate. All incidents, regardless of response time, require thorough documentation to support post-incident analysis and ongoing improvement.

Incident Documentation Requirements:

A comprehensive record of all security incidents is essential. This includes a timeline of incidents with timestamps, details of affected systems and accounts, actions taken along with the rationale, and an assessment of the financial impact. It also involves conducting a root cause analysis, implementing remediation steps, and documenting lessons learned. Procedure updates should be made accordingly. Communication with stakeholders and regulatory notifications, such as those required by the Securities and Exchange Commission (SEC), should be included when applicable. Maintaining such records supports transparency, accountability, and continuous improvement in security management within the digital asset space.

Inadequate recordkeeping transforms routine examinations into significant issues. The inability to produce requested documents within reasonable timeframes signals potential control weaknesses regardless of underlying compliance. Every material decision, trade, and approval should be retrievable with sufficient context to understand the rationale and authorization. Best practice is establishing clear retention requirements by document type, maintaining centralized or well-indexed repositories, and periodically testing retrieval capability. A useful exercise: select a random trade from six months ago and time how long complete documentation takes to assemble. If retrieval exceeds a few hours, recordkeeping processes may warrant enhancement.

5.6 OPERATIONAL COVERAGE & STAFFING

Building an operational team for digital asset management requires addressing the unique demands of 24/7 global markets, heightened technical complexity, and evolving regulatory requirements. The staffing model must balance cost efficiency with the need for continuous oversight to prevent single points of failure.

5.6.1 CORE OPERATIONAL ROLES

The operational structure must provide comprehensive coverage of critical functions. Unlike traditional finance, digital asset markets offer no downtime for weekends or holidays, necessitating models that support 24/7/365 activity.

TABLE 6: REQUIRED OPERATIONAL FUNCTIONS

Role	Primary Responsibilities	Required Skills	Coverage Model
Head of Operations	Strategy, vendor management, process design, regulatory compliance	Operations leadership, crypto expertise	Business hours + on-call

Role	Primary Responsibilities	Required Skills	Coverage Model
Trading Operations	Trade execution, venue management, reconciliation, exception handling	Exchange operations, order management	24/7 shift coverage or extended hours
Settlement & Reconciliation	Daily reconciliation, break resolution, NAV support	Attention to detail, data analysis	Business hours with extended hours during critical periods
Risk Operations	Limit monitoring, exposure calculation, alert response	Risk systems, quantitative skills	Follow-the-sun or on-call model
DeFi Operations	Protocol interaction, smart contract management, yield optimization	DeFi expertise, technical understanding	Business hours with on-call for emergencies

Cross-Training & Resilience:

Cross-training across functions provides flexibility and mitigates key person risk. While operations staff should understand trading systems for emergency support, and trading staff must comprehend operational workflows, segregation of duties must remain intact. Fiduciaries must document formal backup procedures and deputy assignments to ensure continuity during planned or unplanned absences.

5.6.2 24/7 COVERAGE MODELS

Follow-the-Sun Model:

Teams are distributed across time zones (e.g., Asia, Europe, Americas) to provide natural 24-hour coverage.

- *Advantages:* Reduces staff burnout and enables global recruitment.
- *Challenges:* Requires rigorous handoff protocols and high coordination overhead.

Shift-Based Coverage:

Rotating schedules within a single location (e.g., 8am–8pm and 8pm–8am).

- *Advantages:* Simpler communication and unified process standards.
- *Challenges:* Risk of shift-work burnout and higher compensation requirements.

Hybrid Model:

Core hours are handled in a primary location, while follow-the-sun or on-call rotations manage overnight monitoring and alerts. This often leverages automation for routine overnight tasks and is common for mid-sized firms.

5.6.3 SEGREGATION OF DUTIES

Separating roles within operational processes is an essential fiduciary control to prevent fraud and minimize manual errors.

Essential Segregations:

- Trade initiation separated from trade approval (portfolio manager initiates, risk manager or COO approves material trades)
- Withdrawal initiation separated from approval (operations initiates, executive approves)
- Reconciliation performed by person independent of trading
- NAV calculation performed independently of portfolio management
- System administration separated from financial transaction authority

Monitoring Segregation Effectiveness:

Fiduciaries must conduct regular reviews to ensure these separations hold. This includes quarterly access audits, documentation of override justifications, and rotating duties to prevent entrenchment in sensitive roles. Any temporary reassignments for backup coverage must be strictly documented.

Perfect 24/7 coverage is expensive and often unnecessary for most strategies. Analyze actual operational needs: when do most trades occur, what are critical monitoring windows, which protocols require active management. Design coverage around actual requirements, not theoretical ideals. Use automation and alerts to extend human coverage. Maintain on-call procedures for true emergencies rather than staffing for every possibility. Allocators understand coverage constraints but expect: "We maintain extended hours coverage 6am-midnight ET with on-call rotation overnight. Critical alerts route to on-call personnel. Emergency procedures documented for rapid response."

5.7 SETTLEMENT AND RECONCILIATION

Settlement and reconciliation are critical workflows that ensure internal ledgers align with custodian records, counterparty statements, and the immutable state of the blockchain. These processes serve as primary controls to prevent operational losses resulting from manual errors, unauthorized transactions, or counterparty failures. Unlike traditional markets where central clearing allows for reversed settlements, digital asset transactions are instantaneous and irreversible. Consequently, fiduciaries must implement rigorous pre-settlement controls and continuous reconciliation to manage these unique risks effectively.

5.7.1 SETTLEMENT PROCESS

Digital asset settlement typically follows a pre-funded model where assets transfer before trade confirmation, introducing unique risks that require systematic oversight:

- *Pre-Settlement Controls:* A formal approval process for all settlements that evaluates counterparty creditworthiness and historical execution performance. Fiduciaries must assess settlement amounts relative to established counterparty limits and explore alternative execution options to minimize risk. Material transfers should require acceptable collateral or institutional guarantees.
- *Settlement Monitoring:* Real-time tracking of transaction status to confirm asset delivery to the counterparty or receipt of purchased assets. Monitoring must verify that settlement timeframes remain within expected ranges and trigger immediate investigations into any delayed or failed transfers.

- *Settlement Netting:* Wherever feasible, utilize netting to reduce the volume of on-chain transactions and counterparty exposure. Effective netting requires formal legal agreements, rigorous reconciliation of netted amounts, and a clear audit trail for both gross and net settlements.

5.7.2 RECONCILIATION PROCEDURES

Systematic reconciliation identifies discrepancies between internal records and external data sources to enable rapid correction:

- *Daily Position Reconciliation:* Comparison of internal position records against custodian statements, exchange balances (via API), and the direct blockchain state (via node queries). Discrepancies must be investigated and resolved within the same business day, with full documentation of the resolution.
- *Transaction Reconciliation:* Granular matching of every trade across internal systems, exchange confirmations, and on-chain transaction hashes. Any unmatched items must be flagged immediately for investigation. Monthly reports should summarize all breaks and their eventual resolutions to identify systemic issues.
- *Cash Reconciliation:* Continuous alignment of cash positions across traditional banks, stablecoin holdings, and exchange balances. Fiduciaries must verify that every cash movement has corresponding business documentation. Monthly bank statement reviews should include a detailed variance analysis.
- *NAV Reconciliation:* Independent verification that the fund administrator's Net Asset Value (NAV) calculations match internal records. This includes a thorough comparison of position quantities, pricing sources, and underlying calculation methodologies. All NAV "breaks" must be resolved before any reporting is distributed to investors.

5.8 BUSINESS CONTINUITY AND DISASTER RECOVERY

Business continuity planning (BCP) is a foundational requirement for managing operational disruptions, including personnel shortages, technology failures, and natural disasters. In the digital asset space, fiduciaries must address unique failure modes, such as the recovery of custody keys, response protocols for exchange outages, and emergency exit procedures for smart contracts. Maintaining clear communication channels during periods of extreme market

stress is equally vital. Because untested plans are effectively useless during a genuine crisis, ongoing review and rigorous improvement are essential for safeguarding client assets and ensuring operational resilience.

- *Critical Function Identification:* Firms must identify operations essential to the business, including trading capabilities, position monitoring, and cash management. This also encompasses maintaining custody access, investor communications, and regulatory reporting. For each identified function, fiduciaries must determine the maximum acceptable downtime to prioritize recovery efforts.
- *Recovery Procedures:* Step-by-step restoration protocols must be documented, covering system recovery sequences, data restoration from backups, and the activation of alternative execution venues. These procedures should also detail manual processing workarounds and escalation protocols. Documentation must be sufficiently clear that non-experts can execute the instructions during an emergency.
- *Testing Requirements:* Firms must conduct an annual full-scale BCP test that simulates various disruption scenarios. Detailed documentation of these tests is mandatory and must include the scenario description, the procedures executed, and any issues identified. It must also record the time required to restore operations and the lessons learned to inform plan updates. The Board of Directors must receive these results and monitor the status of any required remediation.

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional allocators assess investment operations based on execution quality, reconciliation processes, and operational controls. Demonstrating effective execution analysis, providing daily reconciliation reports, and clearly explaining procedures for interacting with DeFi platforms are essential. These practices indicate a robust operational infrastructure necessary for sound fiduciary management in digital assets.

Trading Infrastructure and Execution

- Describe your trading infrastructure and technology stack. Provide architecture diagram showing systems, connectivity, and redundancy.
- Walk through your best execution policy. Show most recent TCA report demonstrating execution quality analysis.

- How do you manage exchange and venue relationships? What is your execution approach in fragmented multi-venue markets?
- How do you handle DeFi protocol interactions and what controls govern smart contract interactions?
- How do you ensure 24/7 operational coverage?

Reconciliation and Controls

- What is your process for reconciling positions and how often is it performed? Provide sample daily reconciliation report.
- How quickly are reconciliation breaks investigated and resolved?
- What controls prevent unauthorized withdrawals? How do you protect against MEV and sandwich attacks?
- How do you handle exchange outages or blockchain network failures?

Business Continuity

- Can I see your Business Continuity Plan and results of your most recent test?
- What backup procedures exist for each critical function?
- Walk through a recent operational incident and your response.

Documentary Evidence Requirements

- Trading infrastructure documentation and architecture diagrams
- Best Execution Policy and venue evaluation matrix
- Recent TCA reports and execution quality analyses
- Wallet Management and Smart Contract Interaction policies
- Daily reconciliation reports with break resolution documentation
- Business Continuity Plan and recent test results with after-action reports
- Incident logs with root cause analysis
- Security audit and penetration test reports
- Key management procedures and recovery test results
- 24/7 coverage schedules and on-call records

COMMON PITFALLS AND REMEDIATION

- *Manual processes and single-venue dependency*. Trading relies on spreadsheets and one exchange, creating operational fragility and concentration risk. When that venue has issues, operations halt. Remediation: Invest in execution infrastructure supporting multiple venues with automated order routing, position tracking, and reconciliation. Build redundancy before it's needed urgently.
- *Best execution undocumented*. Trades execute without recorded rationale for venue selection, timing, or execution method—making it impossible to demonstrate fiduciary compliance. Remediation: Implement systematic documentation capturing venue analysis, execution rationale, and periodic transaction cost analysis. If you can't explain why a trade was executed the way it was, the process needs improvement.
- *DeFi protocols used without due diligence*. New protocols deployed to production based on yield or opportunity without security review, audit assessment, or governance analysis. Remediation: Establish formal protocol approval requiring: minimum two independent audits, TVL and track record thresholds, governance concentration review, and ongoing monitoring for incidents affecting similar protocols.
- *Reconciliation is periodic, not daily*. Positions reconciled monthly or quarterly—breaks compound undetected, errors persist, fraud risk increases. Remediation: Reconcile all positions and cash daily against independent sources. Establish break aging thresholds with escalation requirements—any item unresolved beyond three days requires senior attention.
- *Incident response is ad hoc*. Security or operational incidents handled reactively without defined roles, escalation paths, or communication protocols. Each incident reinvents the response. Remediation: Document incident response procedures covering: classification criteria, escalation matrix, communication protocols, and post-incident review requirements. Test annually through tabletop exercises.
- *Weak custody and access controls*. Single-signature wallets, shared credentials, or inconsistent authorization procedures expose assets to unauthorized transactions—whether from external compromise or internal misconduct. Remediation: Require multi-signature or MPC for all material holdings. Enforce unique credentials with no sharing. Implement tiered approval matrix by transaction size with time delays and address whitelisting for large transfers.

- *Counterparty exposure unmonitored*. Exchange and protocol balances accumulate without tracking, limits, or creditworthiness assessment—concentration discovered only after counterparty failure. Remediation: Implement real-time counterparty exposure monitoring with concentration limits by venue. Conduct periodic creditworthiness reviews. Reduce exposure before limits are breached, not after.
- *Multi-chain operations lack chain-specific procedures*. Same processes applied across blockchains with different confirmation times, gas dynamics, and risk characteristics—leading to failed transactions, stuck funds, or unexpected costs. Remediation: Document operational procedures for each chain covering: confirmation requirements, gas/fee optimization, bridge risks, and chain-specific failure modes.
- *Staking ignores liquidity constraints*. Portfolio staked without modeling unbonding periods against redemption obligations—assets locked when liquidity is needed. Remediation: Model liquidity requirements accounting for unbonding periods across all staked positions. Maintain unstaked reserves sufficient to meet redemption terms. Document staking allocation decisions with liquidity analysis.
- *Key recovery untested*. Recovery procedures documented but never executed—assumptions about access, timing, and coordination unvalidated until actual emergency. Remediation: Conduct recovery drills at least annually, testing various failure scenarios (key holder unavailable, hardware failure, geographic inaccessibility). Update procedures based on drill findings.
- *24/7 market coverage inadequate*. Trading and risk monitoring designed for traditional market hours while crypto markets operate continuously—incidents occur during coverage gaps. Remediation: Design coverage model matching strategy requirements. Implement automated monitoring with alerting for off-hours. Establish on-call procedures for incidents requiring human intervention.

KEY CONTROLS AND DOCUMENTATION

Document	Purpose	Update Frequency	Owner
Operations Manual	Comprehensive guide to all operational processes, controls, cash movements, reconciliation, onboarding, and provider oversight	Annual or after major changes	Chief Operating Officer
Trading Manual	Procedures for trading and venue workflows	Quarterly	Head of Trading
Best Execution Policy	Execution standards and venue methodology	Annual	CCO/COO
Multi-Chain Operations Guide	Multi-Chain Operations Guide	Quarterly	DeFi Ops Lead
Settlement Framework	Settlement and reconciliation processes	Quarterly	Ops Manager
Incident Plan	Crisis response and escalation protocols	Semi-annual	COO
System Docs	Tech specs, APIs, integrations	Ongoing	CTO
Control Framework	Limits, controls, monitoring	Quarterly	Risk/Ops
Vendor Docs	Exchange and provider agreements	Annual	Legal/Ops
Trade Blotter	Record of all trades	Daily	Ops Team
Reconciliation Reports	Position, balance, P&L checks	Daily	Ops Team
Incident Log	Issues and resolutions	Ongoing	Ops Manager
Coverage Schedule	24/7 staffing and on-call rotation	Monthly	Ops Manager

STANDARD 6: RISK MANAGEMENT

Firms must implement comprehensive risk management. This includes an enterprise-wide risk management framework covering all material risks—market, credit, operational, liquidity, and technology—with appropriate measurement and monitoring methodologies. Firms must conduct regular stress testing and scenario analysis programs calibrated to portfolio characteristics, define risk limits with clear escalation and remediation procedures for breaches, and maintain a board-approved risk appetite statement with regular review and updates.

Managing risks in digital assets requires frameworks that address both traditional financial risks and emerging threats unique to this market. These specific threats include smart contract vulnerabilities, protocol failures, attacks on consensus mechanisms, custody breaches, and regulatory uncertainties that may challenge the very existence of certain digital assets. Traditional tools, such as Value-at-Risk (VaR), are often inadequate due to the extreme volatility and potential for "fat-tail" market movements. During periods of market stress, asset correlations frequently break down and standard liquidity assumptions often fail as liquidity can vanish across multiple trading venues simultaneously.

Standard 6 emphasizes the implementation of comprehensive enterprise risk management (ERM). This involves identifying significant risks across market, credit, operational, liquidity, and technology domains. To ensure integrity, risk management functions must operate independently from investment teams, serving to challenge investment decisions rather than merely validate them. Quantitative risk metrics must be supplemented by qualitative assessments to capture risks that are difficult to measure numerically. Furthermore, fiduciaries must conduct regular stress testing using crypto-specific scenarios and maintain risk limits that effectively constrain behavior. When limits are breached, automatic escalation processes must be in place to address issues promptly.

Effective risk management serves as an independent "challenge function" rather than a checkbox exercise for portfolio teams. Stress testing must reflect the unique market structure and potential failure modes of digital assets, supported by clear procedures for escalation when risk limits are exceeded. Documentation of risk-related decisions should demonstrate a consistent approach to applying established frameworks. Fiduciaries must accept that constraining profitable opportunities is sometimes necessary when risk-adjusted returns are inadequate. Treating risk management as a compliance formality rather than a core value-

protection function can lead to failures in meeting institutional standards, regardless of a firm's past performance.

6.1 ENTERPRISE RISK MANAGEMENT FRAMEWORK

Enterprise Risk Management (ERM) provides a top-down, firm-wide approach to identifying, assessing, and managing risk. ERM establishes the governance structures, policies, and processes necessary to ensure consistent risk treatment across all firm activities. An effective ERM program is distinguished by its independence from business pressures, a comprehensive risk taxonomy covering all material threats, and the use of quantitative metrics supplemented by qualitative judgment. Furthermore, it must include clear escalation procedures that activate whenever risks exceed established tolerances.

6.1.1 RISK GOVERNANCE

Effective risk governance is built on the "three lines of defense" model, which separates risk-taking from monitoring and independent assurance:

- *First Line of Defense:* The investment team and business units bear the primary responsibility for risk-taking and day-to-day management. Portfolio managers make decisions within set limits, operations teams execute transactions according to approved procedures, and business development stays within strategic boundaries. While the first line "owns" the risk, it requires independent oversight to prevent conflicts between performance incentives and sound risk management.
- *Second Line of Defense:* The risk management function provides independent oversight and acts as a challenge to the first line. Key responsibilities include developing risk frameworks and policies, calculating risk metrics, and monitoring limits. The second line is responsible for challenging investment decisions when the risk-reward profile appears inadequate, escalating breaches, and reporting the firm's risk status to senior management and the board. Independence is critical; the risk function must never report to the individuals whose activities it is required to monitor.
- *Third Line of Defense:* Internal audit provides independent assurance that the risk framework is functioning effectively. Audit reviews verify whether policies reflect actual practice, if limits are monitored and breaches addressed, and if reporting provides an accurate picture of firm risk. It also assesses the effectiveness of

control testing. Findings from the third line are reported directly to the board's audit committee, independent of management.

The Chief Risk Officer (CRO)

Firms should maintain a dedicated Chief Risk Officer (CRO) who is independent of the investment team and reports directly to the CEO or the board. The CRO's authority includes:

- Approving risk policies and limits.
- Challenging investment decisions that exceed risk tolerances.
- Halting activities that create unacceptable levels of risk.
- Escalating material risk issues directly to the board.

To preserve this independence, the termination of a CRO should require board notification or approval. Management's unilateral ability to remove a CRO eliminates the necessary independence required when risk management priorities challenge business growth ambitions.

6.1.2 RISK APPETITE STATEMENT

A Risk Appetite Statement is a board-approved document that defines the specific types and amounts of risk a firm is willing to accept in pursuit of its objectives. To be effective, this statement must translate high-level qualitative goals into quantitative limits that allow for objective measurement and continuous monitoring. Generic phrases such as "appropriate risk management" or "prudent risk-taking" fail to provide the operational guidance required for fiduciary-grade management.

The statement must explicitly address the following five areas:

- *Market Risk Tolerance:* Establishment of specific numerical limits to enable objective compliance verification. This includes defining maximum portfolio volatility, drawdown limits, Value-at-Risk (VaR) thresholds, and concentration limits categorized by position and sector.
- *Credit Risk Tolerance:* Definition of counterparty exposure limits based on creditworthiness. This includes setting boundaries for aggregate exchange exposure, unsecured lending limits, and specifying acceptable collateral types along with their required haircuts.
- *Liquidity Risk Tolerance:* Requirements for maintaining minimum liquidity reserves and limiting the concentration of illiquid positions. The statement must also define required redemption capacity under various stress scenarios and acceptable time horizons for position liquidation.

- *Operational Risk Tolerance:* Specifications regarding the acceptable frequency and severity of operational losses. It must establish standards for the control environment, define recovery time objectives (RTOs) for business continuity, and set a tolerance level for cybersecurity incidents.
- *Technology Risk Tolerance:* Criteria for interacting with smart contracts and specific security requirements for protocols. This also includes establishing minimum system uptime standards and defining the firm's disaster recovery capabilities.

A Risk Appetite Statement provides value only when translated into specific, measurable limits. Qualitative statements like "low appetite for counterparty risk" enable any exposure to be rationalized as acceptable. Effective risk governance requires numerical limits that create clear boundaries and trigger defined escalation procedures when approached or breached. Best practice is establishing a limit framework that cascades from board-approved risk appetite to specific position, counterparty, and concentration limits with defined monitoring frequency and breach response procedures. The framework should be calibrated so limits occasionally bind during normal operations—if no limit is ever approached, they may be set too loosely to provide meaningful constraint.

6.2 DIGITAL ASSET RISK TAXONOMY

A risk taxonomy provides a structured framework for identifying and categorizing all material risks. A comprehensive digital asset taxonomy must address traditional financial risks alongside crypto-specific threats. The completeness of this taxonomy determines whether risk management captures all material exposures or focuses too narrowly on easily quantified market risks while neglecting operational and technology threats that could cause significantly larger losses.

TABLE 1: RISK TAXONOMY

Risk Category	Key Components
Market Risk	Price volatility, concentration risk, correlation breakdown, basis risk, liquidation cascades, market manipulation, regime changes, stablecoin de-pegging.
Credit Risk	Exchange insolvency, counterparty default, lending protocol failures, collateral shortfalls, settlement failures, custodian bankruptcy, prime broker concentration.
Liquidity Risk	Market liquidity evaporation, funding liquidity stress, redemption capacity shortfalls, forced liquidations, position illiquidity, exchange withdrawals suspended, bank runs.
Operational Risk	Execution errors, reconciliation failures, custody key loss, unauthorized transactions, fraud, process failures, personnel errors, system outages, vendor failures.
Technology Risk	Smart contract exploits, protocol vulnerabilities, consensus attacks, blockchain reorganizations, oracle failures, bridge hacks, wallet compromises, cybersecurity breaches.
Regulatory Risk	Classification changes, enforcement actions, jurisdiction restrictions, compliance failures, registration requirements, reporting obligations, sanctions, cross-border restrictions.

Risk frameworks often fail when traditional taxonomies are applied without crypto-specific extensions. Market and credit risk models designed for traditional assets may miss smart contract vulnerabilities, protocol governance risks, oracle manipulation, bridge exploits, and MEV extraction. A comprehensive risk taxonomy must address both traditional financial risks and threats unique to digital assets. Best practice is developing a taxonomy that explicitly includes digital asset-specific risk categories: smart contract/protocol risk, custody/key management risk, blockchain/network risk, and counterparty risks specific to crypto infrastructure (exchanges, stablecoins, DeFi protocols). Each category should have defined identification, measurement, and monitoring approaches appropriate to its characteristics.

6.3 RISK MEASUREMENT AND QUANTIFICATION

Risk measurement translates qualitative assessments into quantitative metrics, enabling objective monitoring and the enforcement of limits. This quantification allows fiduciaries to compare potential impacts across diverse risks, track trends over time, and make informed trade-offs between risk and return. However, over-reliance on these metrics can create false precision; many critical risks resist quantification and require qualitative judgment to supplement numerical analysis.

6.3.1 MARKET RISK METRICS

No single metric can capture all dimensions of market risk; comprehensive measurement requires multiple complementary approaches to quantify potential losses from adverse price movements:

- *Value at Risk (VaR):* VaR is a statistical measure of potential loss over a defined period at a specific confidence level (e.g., a daily 95% VaR of $1M indicates 95% confidence that daily losses will not exceed $1M). While VaR provides a single summary number, it has limitations: it assumes normal distributions (understating tail risk), uses historical data that may not predict the future, and provides no information on loss severity beyond the threshold. Digital asset VaR requires short lookback periods to capture current volatility, the inclusion of stress periods, and supplementation with scenario analysis.
- *Stress Testing:* This involves simulations to assess portfolio impact under extreme but plausible scenarios. Crypto-specific stress scenarios should include major

exchange failures, regulatory crackdowns, stablecoin collapses cascading through DeFi, consensus attacks, or correlated liquidation cascades. Stress testing identifies vulnerabilities missed by statistical measures, such as exchange concentration or correlation breakdowns under pressure.

- *Scenario Analysis:* A forward-looking exercise assessing the impact of specific hypothetical events. Scenarios should consider historical precedents, systemic market vulnerabilities, regulatory shifts, and technology failure modes. These must be updated quarterly to reflect evolving threats.
- *Concentration Metrics:* Fiduciaries must track position, sector, liquidity, counterparty, and protocol concentration. Tools like the Herfindahl index should be used to quantify diversification. Specific concentration limits are necessary to prevent a portfolio from being dominated by a single exposure.

6.3.2 OTHER RISK METRICS

Beyond market risk, firms must implement Key Risk Indicators (KRIs) to provide early warning signals across all material risk categories:

- *Credit Risk KRIs:* Monitoring exchange exposure versus limits, counterparty credit ratings, margin utilization, collateral coverage ratios, and days to liquidate counterparty exposures.
- *Liquidity Risk KRIs:* Tracking days to liquidate the portfolio, redemption capacity under stress, diversity of funding sources, and stablecoin concentration.
- *Operational Risk KRIs:* Measuring the frequency of failed trades, reconciliation breaks, unauthorized transaction attempts, key person dependencies, and audit findings.
- *Technology Risk KRIs:* Monitoring system uptime, cybersecurity incidents, vulnerability scan results, patch management status, and protocol audit age.

Common mistakes in risk management include overreliance on a single metric like VaR. While VaR offers useful summary data, it has notable limitations in digital asset markets. It assumes returns follow a normal distribution, which understates tail risk. It also relies on historical data that may not predict future risks and provides no insight into potential losses beyond the VaR threshold. Investment managers should request a comprehensive set of risk metrics, including calculation methods, stress testing scenarios and results, correlation assumptions, and analysis of risk under stress conditions. Relying solely on VaR without incorporating stress tests, scenario analysis, and concentration metrics can lead to inadequate risk assessment. During due diligence, a key question is to review the worst daily loss in the past year and determine if risk metrics predicted that loss. If not, it indicates a need to improve risk measurement practices. Proper risk assessment involves a thorough understanding of potential losses and the limitations of the metrics used, ensuring a more robust approach to digital asset risk management.

6.4 RISK MONITORING AND REPORTING

Risk monitoring tracks exposures over time to identify trends, breaches, and emerging threats. Effective monitoring relies on real-time data feeds for immediate breach detection, automated alerting to prevent oversight, and visualization dashboards for pattern recognition. Risk reporting communicates this status to decision-makers to enable informed responses; its value depends on clarity and actionability. Comprehensive reports that bury key messages in excessive detail are ineffective, regardless of their technical sophistication.

6.4.1 RISK DASHBOARD

The risk dashboard provides a daily or weekly overview of critical exposures and is distributed to the CIO, CEO, and Risk Committee. To support fiduciary responsibilities, the dashboard must remain concise, focused, and easy to interpret. The primary goal is to facilitate proactive risk management through timely, relevant information.

- *Market Risk Summary:* Portfolio Value at Risk (VaR), stress test results, and position concentration. It also tracks largest exposures and volatility trends compared to historical ranges and established limits.
- *Credit Risk Summary:* Counterparty exposure by entity and concentration metrics. This includes monitoring credit quality distribution, margin utilization, and "near-limit" situations.

- *Liquidity Assessment:* An overview of the portfolio liquidity profile and days required to liquidate positions. It also monitors redemption capacity, cash reserves, and funding source stability.
- *Limit Breaches:* A record of all current limit violations, including the magnitude and duration of the breach. It must document the remediation timeline and the specific party responsible for resolution.
- *Key Risk Indicators (KRIs):* Trends across operational, technology, and regulatory risk categories. Thresholds requiring immediate management attention must be clearly highlighted.

6.4.2 RISK COMMITTEE

The Risk Committee provides board-level oversight of the firm's enterprise risk management program. Meeting at least quarterly, the committee reviews risk appetite compliance, limit breach remediation, stress testing results, and emerging threats. The committee must include independent directors with risk management expertise and a Chief Risk Officer (CRO) who presents assessments independently of management. The committee must hold the authority to escalate material concerns directly to the full board.

6.5 RISK MITIGATION AND CONTROLS

Risk mitigation reduces exposure through internal controls, risk transfer to third parties, or the elimination of high-risk activities. Control effectiveness determines whether risks stay within tolerances or result in actual losses. While insurance or contracts can shift financial burdens, they do not eliminate the firm's ultimate responsibility for risk management.

6.5.1 INTERNAL CONTROLS

Internal controls are the policies and systems designed to mitigate risk within daily operations.

- *Segregation of Duties:* Separating trade execution, settlement, and custody functions. This prevents a single individual from initiating and completing transactions without independent verification.
- *Access Controls:* Restricting access to systems and data based on "need-to-know" principles. Controls include multi-factor authentication (MFA), regular access reviews, and privileged access monitoring.

- *Reconciliation:* Daily reconciliation of cash and positions across all sources. Any discrepancies must be investigated immediately by a function separate from operations.
- *Authorization Hierarchies:* Defined approval requirements based on the materiality of a transaction. All authorizations must include documented business rationales, and overrides are prohibited without formal escalation.
- *Monitoring and Alerts:* Systems that provide real-time notification when key metrics hit threshold levels. Formal escalation procedures must be in place for critical alerts.

6.5.2 RISK TRANSFER

Risk transfer involves shifting the financial burden of potential losses to third parties. This does not, however, replace the firm's duty to manage those risks proactively.

- *Insurance:* Standard policies for crime (fraud/theft), cyber security, D&O (governance failures), and E&O (professional liability). Fiduciaries should seek digital asset-specific policies for custody losses, smart contract failures, or exchange insolvencies.
- *Contractual Protections:* Negotiating indemnifications from service providers, liability limitations, and insurance requirements for counterparties. This may also include parent company guarantees.
- *Hedging:* Utilizing derivatives to reduce market risk exposure. Common strategies include basis risk hedging, tail risk protection through options, and correlation hedges.

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional allocators evaluate risk management through framework comprehensiveness, measurement rigor, and control effectiveness. Inability to demonstrate systematic risk identification, produce real-time monitoring dashboards, or explain limit breach procedures reveals inadequate enterprise risk management.

Risk Framework and Governance

- Walk through your risk management framework. How do you systematically identify emerging risks in digital assets?

- Who is your CRO and what is their background? Can I see your Risk Appetite Statement?
- Provide Risk Committee charter and redacted minutes from recent meeting showing discussion depth and decisions.
- How frequently do you update comprehensive risk assessments?

Risk Measurement and Monitoring

- What specific risk metrics do you track across market, credit, operational, liquidity, and technology risk categories?
- How do you adapt traditional metrics like VaR for cryptocurrency characteristics?
- Walk through your scenario analysis and stress testing approach. Show recent stress testing results.
- Show your actual risk monitoring dashboard currently in production use. What do you monitor in real-time versus daily?
- What are your current actual risk levels across key metrics?

Risk Controls and Mitigation

- What are your primary risk control mechanisms? How do you implement position and portfolio limits operationally?
- Describe a recent significant risk event and your response. What is your single largest risk exposure currently and why is it acceptable?
- How do you manage concentration risks systematically?
- What insurance do you maintain and what does it cover? Provide copy of insurance policies.

Documentary Evidence Requirements

- Complete ERM Framework document and Risk Appetite Statement
- Risk Committee charter and meeting minutes for past 6-12 months
- Current daily, weekly, and monthly risk reports
- Sample risk monitoring dashboard showing real-time metrics
- Recent stress testing results with scenario descriptions
- Incident logs documenting events and responses
- Limit breach documentation with approvals and remediation
- Control testing documentation and results

COMMON PITFALLS AND REMEDIATION

- *Risk function lacks independence*. Risk management reports to the CIO or investment team, compromising ability to challenge positions or escalate concerns. Risk becomes advisory rather than authoritative. Remediation: Establish CRO reporting to CEO or board with direct board access. Risk function should have authority to enforce limits without investment team approval. Independence is demonstrated through documented instances of challenge—if risk never disagrees with the portfolio, it's not functioning independently.
- *Limit breaches tolerated without consequence*. Limits exist on paper but breaches are routinely accepted, extended, or explained away. Limits that don't bind provide no risk control. Remediation: Implement automated breach detection with immediate escalation. Require written approval with rationale and remediation timeline for any extension. Track all breaches and resolutions—patterns of repeated breach-and-extend indicate limits set incorrectly or culture that doesn't respect boundaries.
- *Stress testing uses generic scenarios*. Stress tests apply traditional market drawdowns (20-30%) when crypto routinely experiences 50%+ declines, or miss crypto-specific events entirely. Results provide false comfort. Remediation: Develop scenario library reflecting digital asset realities: major exchange failure, stablecoin depegging, regulatory enforcement action, protocol exploit, and correlated liquidation cascades. Scenarios should be severe enough to reveal vulnerabilities.
- *Risk measurement relies solely on VaR*. Value-at-Risk as the primary metric understates tail risk in fat-tailed crypto return distributions. VaR tells you little about what happens in the scenarios that matter most. Remediation: Supplement VaR with scenario analysis, maximum drawdown analysis, liquidity stress testing, and concentration metrics. Report multiple measures—no single metric captures digital asset risk adequately.
- *Risk reporting obscures rather than clarifies*. 50-page daily reports bury critical information in detail. Decision-makers can't quickly identify what requires attention. Remediation: Implement tiered reporting: one-page executive dashboard highlighting limit utilization, concentration, stress results, and items requiring action—with detailed supporting analysis available separately. If a board member can't assess risk posture in five minutes, reporting needs simplification.

- *Risk committee provides no meaningful oversight.* Committee reviews reports and approves recommendations without substantive discussion. Minutes show unanimous approval with no recorded debate. Remediation: Include independent members with risk expertise. CRO should present directly, not through CIO. Minutes must document questions raised, concerns discussed, and rationale for decisions. A committee that never challenges management isn't governing.
- *Risk controls documented but untested.* Limits, escalation procedures, and risk responses exist in policy but haven't been validated operationally. Assumptions about how controls work may not hold under stress. Remediation: Test key controls periodically—verify limit monitoring catches breaches, escalation procedures reach the right people, and response protocols work as designed. Present testing results to risk or audit committee.
- *Counterparty exposure fragmented and unmonitored.* Exposure to exchanges, lenders, and protocols tracked separately or not at all. Aggregate counterparty concentration unknown until failure reveals it. Remediation: Centralize counterparty exposure reporting across all venues and instruments. Implement concentration limits by counterparty. Conduct periodic credit quality assessment—particularly for exposures that have grown material through market movements.
- *Losses occur without post-mortem analysis.* Loss events and near-misses aren't systematically analyzed for lessons. Same failures repeat because root causes aren't identified or addressed. Remediation: Require formal post-incident review for material losses and significant near-misses. Document what happened, why controls didn't prevent it, and specific remediation actions. Track remediation to completion—the value is in changes made, not reports written.

KEY CONTROLS AND DOCUMENTATION

Document Category	Specific Purpose	Required Update Frequency	Primary Ownership
Risk Management Policy	Comprehensive risk framework, Governance structure definition, Roles and responsibilities	Annual comprehensive review with interim updates for material changes	CRO/CEO jointly
Risk Appetite Statement	Approved risk tolerance, Quantitative limit specifications, Qualitative boundary guidance	Annual review or after material events	Risk Committee
Risk Register	Enterprise risk inventory, Impact and likelihood assessment, Control and mitigation documentation	Monthly comprehensive update with continuous additions	Risk Management Team
Risk Measurement Methodology	Detailed calculation procedures, Assumptions and limitations, Model validation results	Quarterly review with updates after methodology changes	Senior Risk Analyst
Risk Limit Framework	Complete limit hierarchy, Trigger and escalation procedures, Approval authority matrix	Monthly review ensuring current alignment	Risk Committee
Stress Testing Framework	Scenario definitions and assumptions, Execution procedures and timing, Results interpretation guidance	Quarterly review with market evolution updates	Senior Risk Analyst

Document Category	Specific Purpose	Required Update Frequency	Primary Ownership
Incident Response Plan	Crisis identification and classification, Escalation and communication protocols, Recovery procedures	Semi-annual review with post-incident updates	COO and CRO jointly
Risk Reporting Standards	Report templates and formats, Distribution lists and protocols, Escalation procedures	Quarterly review ensuring continued relevance	Risk Operations Analyst
Limit Breach Log	Chronological breach record, Remediation action documentation, Governance approval evidence	Real-time continuous maintenance	Risk Operations Analyst
Risk Committee Minutes	Meeting deliberations and decisions, Action item assignments, Follow-up tracking	Within 24 hours of each meeting	Committee Secretary

STANDARD 7: LEVERAGE & LIQUIDITY MANAGEMENT

Firms must manage leverage and liquidity prudently. This includes clear leverage policies with ongoing monitoring and controls appropriate to strategy and investor terms; liquidity management aligned with redemption terms and investor obligations; and diversified financing sources and counterparty relationships to reduce concentration risk. Firms must conduct regular stress testing of liquidity and leverage under adverse market conditions and document contingency plans for stressed market conditions including liquidity squeeze scenarios.

Leverage and liquidity in digital assets exhibit a concentrated interdependence: leverage amplifies gains and losses more rapidly than in traditional markets, while liquidity can evaporate across all global venues simultaneously. The 2022 crypto credit crisis brutally demonstrated these dynamics, as overleveraged firms faced margin calls that forced liquidations into illiquid markets, triggering cascading failures among interconnected counterparties. Firms that survived this period maintained conservative leverage, utilized diversified financing sources, and stress-tested their liquidity under extreme scenarios. Conversely, firms that failed often relied on concentrated financing, underestimated correlations during stress, and found their "liquid" positions became unsellable exactly when capital was needed most.

Standard 7 emphasizes the necessity of clear, disciplined management of these risks. Fiduciaries should implement straightforward policies that include real-time tracking of all funding sources to ensure sufficient reserves for redemptions during periods of stress. Diversifying funding sources is essential to avoid reliance on a single provider. Furthermore, regular stress tests using crypto-specific scenarios are required to identify potential vulnerabilities. During crises, standard market assumptions often fail: correlations shift, liquidity providers may withdraw, and funding sources can vanish without notice. Adhering to these rigorous practices is vital for maintaining the stability and resilience of digital asset portfolios.

Upholding this standard requires continuous monitoring of all leverage sources and maintaining diversified financing even when more favorable terms are available from fewer providers. Fiduciaries must accept that conservative leverage limits may restrain returns during bull markets in exchange for long-term stability. While maximizing leverage during favorable conditions may optimize for short-term gains, it creates existential risks during

market stress. Institutional allocators prioritize capital preservation through entire market cycles over maximizing returns in any single period.

7.1 FRAMEWORK FOR LEVERAGE MANAGEMENT

Leverage is the use of borrowed capital to amplify potential investment returns. While it increases gains, it symmetrically magnifies losses, carrying the inherent danger that a decline can exceed invested capital and trigger forced liquidations. A disciplined leverage framework prevents excessive risk-taking during favorable markets while maintaining tactical flexibility. The effectiveness of this framework depends on identifying all leverage sources, real-time monitoring, clear behavioral limits, and stress testing to reveal vulnerabilities before they result in catastrophic losses.

7.1.1 SOURCES OF LEVERAGE

Digital asset leverage originates from diverse sources, each with distinct risks. Comprehensive management requires identifying implicit leverage—such as that found in derivatives—which is often overlooked in traditional metrics.

- *Prime Brokers:* Crypto-native and traditional providers offer financing, consolidated risk management, and custody. While cost-efficient, prime broker concentration creates systemic risk; correlated margin calls can occur if multiple funds borrow from the same provider. Due diligence must assess their financial stability, margin methodologies, and liquidation timelines.
- *Exchange Margin Trading:* Many venues offer integrated margin trading, providing convenience but introducing significant counterparty risk. Exchange insolvency or hacks can lead to total loss. Monitoring requires real-time tracking of margin utilization and liquidation prices, alongside concentration limits to prevent over-exposure to a single venue.
- *DeFi Lending Protocols:* Protocols like Aave and Maker allow borrowing against collateral without traditional counterparty credit risk. However, they introduce smart contract vulnerabilities, oracle manipulation risks, and aggressive liquidation mechanics. Leverage in DeFi requires auditing contract code, monitoring collateralization ratios, and assessing the impact of gas price spikes on the ability to manage positions.
- *Derivatives (Implicit Leverage):* Futures, perpetual swaps, and options create synthetic leverage. A futures position with 10% margin provides 10x leverage without a loan principal appearing on the balance sheet. This is particularly

dangerous because margin requirements can spike during volatility, and funding rates on perpetuals can turn sharply negative, rapidly increasing the cost of the position.

7.1.2 LEVERAGE LIMITS AND MONITORING

A formal leverage policy defines the firm's approach through specific limits and escalation protocols. This policy must be granular enough to constrain behavior rather than provide a rationalization for opportunistic risk-taking.

- *Gross and Net Exposure Limits:* Maximum gross exposure (sum of long/short) and net exposure (directional bias), expressed as a percentage of NAV. Gross exposure is the primary measure of total operational risk.
- *Leverage Ratio Limits:* Specific ratios of total assets to equity and maximum borrowing caps. Fiduciaries should maintain a minimum equity cushion significantly above exchange or protocol liquidation thresholds.
- *Source Concentration Limits:* Maximum leverage allowed from any single counterparty or protocol. Diversification across financing sources prevents a single provider's failure from jeopardizing the entire fund.
- *Collateral Management:* Minimum collateralization ratios defined by asset type, including specific "haircuts" (valuation discounts) for more volatile assets. Procedures must be in place for immediate response to margin calls.
- *Real-time Monitoring:* Automated systems must calculate leverage across all sources continuously. Alerts should trigger when approaching limits, with clear authority granted to the risk function to reduce leverage within defined timeframes.

Leverage measurement can fail when it captures explicit borrowing but misses embedded exposure in derivatives. A fund reporting 1.5x leverage based on margin loans may have significantly higher effective exposure when including futures and perpetual swap notional. Comprehensive leverage measurement requires aggregating all sources—explicit borrowing and synthetic exposure—across all venues and instruments. Best practice is calculating leverage using a methodology that includes: prime broker margin, exchange margin accounts, DeFi borrowing, and notional exposure from derivatives. This comprehensive measure should be monitored in real-time or at minimum daily, with clear limits and escalation procedures. Understanding true economic exposure is essential for both risk management and accurate investor communication.

7.2 LIQUIDITY MANAGEMENT FRAMEWORK

Liquidity is the ability to divest assets rapidly without inducing a significant adverse price impact. In the digital asset ecosystem, liquidity is highly fragmented across global platforms and can evaporate instantaneously during market stress. Assets that appear liquid during stable periods often become impossible to sell during a crisis—precisely when capital is most urgently needed. Effective management involves rigorous classification, stress testing under extreme scenarios, and maintaining sufficient reserves to meet obligations without resorting to forced liquidations. Fiduciaries must recognize that historical liquidity levels are not always predictive of future availability.

7.2.1 LIQUIDITY PROFILE OF ASSETS

Understanding a portfolio’s liquidity requires classifying assets into "buckets" based on the time required to liquidate them without material price impact. This classification informs position sizing, redemption capacity, and concentration limits.

Trading Volume and Market Depth:

Average daily trading volume (ADV) provides a baseline, but true liquidity is often far lower than headline figures suggest, as volume typically concentrates in a small percentage of total supply. Market depth analysis is essential to examine the order book: how much can be traded at current prices before moving the market? Assets with "thin" order books may show high volume but prove illiquid for institutional-sized positions.

Bid-Ask Spread:

The spread between bid and ask prices indicates the immediate execution cost. While narrow spreads (<0.1%) suggest high liquidity, they can widen dramatically during volatility—an asset with a 0.05% spread in calm markets may experience a 5% spread during stress. Fiduciaries should analyze spread distributions across various market regimes, not just normal periods.

Time to Liquidate:

This metric estimates the days required to exit a position without exceeding a specific price impact threshold (typically 2-5%). It combines volume analysis with position size. For example, a position representing 5 days of ADV, assuming a 10% participation rate, would require 50 days to liquidate.

TABLE 1: ASSET LIQUIDITY TIERS

Tier	Time to Liquidate	Spot Assets	Derivatives
Tier 1 (Highly Liquid)	< 1 day	BTC, ETH, major stablecoins (USDT, USDC). High volume across multiple venues, tight spreads, deep order books	BTC and ETH perpetuals/futures on major exchanges. Deep liquidity, tight spreads, 24/7 execution.
Tier 2 (Liquid)	1-5 days	Large-cap altcoins with consistent volume. Moderate spreads, reasonable depth. Liquidity deteriorates significantly during stress.	Altcoin perpetuals for major assets. Good liquidity in normal markets but funding rates spike and liquidity evaporates during volatility. Position limits may constrain large holdings.
Tier 3 (Moderately Illiquid)	5-30 days	Mid-cap tokens, DeFi governance tokens. Variable volume, wider spreads, thin order books. Requires careful execution to avoid significant impact.	Options on BTC/ETH. Reasonable liquidity near-the-money, deteriorates for out-of-money strikes. Wide bid-ask spreads. Early close requires accepting market price.

Tier	Time to Liquidate	Spot Assets	Derivatives
Tier 4 (Illiquid)	> 30 days	Small-cap tokens, venture positions with lockups, NFTs, LP tokens. Very low volume, large spreads, minimal depth. May require OTC transactions or extended timeframe.	Exotic derivatives, structured products, long-dated options on altcoins. Minimal secondary market. May require holding to expiration or negotiated exit.

Liquidity analysis based solely on normal-market conditions may provide false comfort. Assets appearing liquid during calm periods can become difficult or impossible to exit during stress—precisely when liquidity is needed most. Historical trading volumes may not predict crisis-period executability, particularly in digital asset markets that have experienced multiple severe liquidity dislocations. Best practice is stress-testing liquidity under adverse scenarios that reflect historical digital asset crises: 50%+ market declines, exchange withdrawal freezes, stablecoin depegging, and correlated selling across venues. The analysis should inform both position sizing and redemption terms, ensuring commitments to investors are achievable under stress conditions.

7.2.2 LIQUIDITY STRESS TESTING

Regular liquidity stress testing assesses the firm's ability to meet financial obligations under adverse conditions without resorting to forced asset liquidations at unfavorable prices. These scenarios must reflect digital asset-specific failure modes rather than simply adapting traditional financial assumptions. Testing should occur at least quarterly, with the results directly informing liquidity reserve requirements and redemption policies.

- *Market Downturn Scenario:* This models a simultaneous, sharp decline across all digital assets (50–80% drawdown) where correlations converge toward 1.0 and liquidity contracts across all tiers. The model typically assumes Tier 1 liquidity is halved, Tier 2 drops by 75%, and lower tiers become effectively illiquid. Fiduciaries must calculate the days required to raise cash for redemptions and the total portfolio loss resulting from forced sales.

- *Redemption Shock Scenario:* This simulates large, unexpected redemption requests—typically 25–50% of AUM—concentrated among the largest investors. The test evaluates the ability to meet these requests using only Tier 1 and Tier 2 assets without forced liquidation of illiquid positions. It identifies the timeframe required for orderly liquidation and assesses additional liquidity sources, such as credit lines or asset sales.
- *Counterparty Failure Scenario:* This scenario assumes a major exchange or prime broker failure results in frozen assets for an extended period (3–12 months). The analysis calculates the remaining liquidity available from other sources and the firm's ability to meet redemptions with accessible assets. It also evaluates the impact on leverage ratios, margin requirements, and the costs associated with shifting to alternative execution venues.
- *Stablecoin De-Peg Scenario:* This models a crisis where a major stablecoin loses its peg, triggering a liquidity crunch across the DeFi ecosystem. Managers must assume stablecoin reserves decline 30–50% in value, causing cascading liquidations. The test calculates direct and indirect exposure through DeFi protocols, collateral adequacy in the event of a decline, and the time required to replace compromised stablecoin liquidity with viable alternatives.

Redemption terms mismatched with portfolio liquidity create structural risk. Offering monthly liquidity while holding positions requiring extended periods to exit means redemption requests during stress may force sales that harm remaining investors. The 2022 crypto credit crisis demonstrated how quickly liquidity mismatches can become existential. Best practice is setting redemption terms based on stressed liquidation analysis rather than marketing considerations. The analysis should answer: "If we received redemption requests for a significant portion of AUM during market stress, how specifically would we meet them?" Gate provisions and suspension rights should be clearly documented and calibrated to portfolio characteristics.

7.3 FINANCING AND COUNTERPARTY MANAGEMENT

Financing is a cornerstone of leveraged investment strategies, requiring diverse and stable funding sources to ensure capital access across all market regimes. The 2022 crypto credit crisis illustrated the catastrophic risks of single-lender reliance, as multiple firms lost funding

simultaneously and were forced into "fire-sale" liquidations. Fiduciaries who maintain diversified financing—distributed across multiple lenders, protocols, and jurisdictions—are significantly better positioned to withstand systemic shocks.

7.3.1 DIVERSIFICATION OF FINANCING SOURCES

Firms must reduce reliance on any single provider by diversifying across counterparties, platforms, and mechanisms.

- *Counterparty Diversification:* No single entity should provide more than 30–40% of total borrowing. Fiduciaries should maintain multiple prime broker relationships even if one offers more attractive terms, while regularly assessing each counterparty's financial health and exposure to other leveraged funds.
- *Platform Diversification:* Utilize a strategic mix of centralized exchanges (CeFi), decentralized protocols (DeFi), and traditional prime brokers. This balances CeFi convenience with DeFi transparency and ensures cross-platform operational flexibility.
- *Geographic Diversification:* Distribute financing across multiple jurisdictions to mitigate regulatory risk. This involves balancing U.S.-based entities with offshore alternatives and maintaining a deep understanding of the local legal and bankruptcy frameworks.
- *Mechanism Diversification:* Employ a mix of secured borrowing, unsecured credit lines, repo facilities, and derivatives-based leverage. Pre-arranging credit lines ensures rapid access during periods of stress.

7.3.2 COUNTERPARTY DUE DILIGENCE

Rigorous, ongoing due diligence is required to mitigate the risk of counterparty failure. 2026 institutional standards prioritize transparency and verifiable reserves.

- *Financial Condition:* Review audited financial statements for capitalization adequacy and revenue sustainability. Fiduciaries must monitor regulatory capital compliance and credit ratings while evaluating the counterparty's insurance coverage and recovery mechanisms.
- *Risk Management Practices:* Analyze margin calculation methodologies and liquidation procedures. Due diligence must include an assessment of the counterparty's stress-testing frameworks and their historical loss experience during volatile regimes.
- *Legal and Regulatory Standing:* Verify all jurisdictional licenses and compliance with AML/KYC standards. Essential checks include litigation history, bankruptcy-

remote structures, and the clear segregation of client assets from firm capital—often verified through "Proof of Reserves" attestations.

- *Operational Capabilities:* Evaluate technology security measures and the maturity of business continuity plans. Managers must also consider key person dependencies and review independent audit reports (such as SOC 2 Type II) to ensure operational integrity.

7.3.3 FINANCING COST MANAGEMENT

Effective cost management requires a granular understanding of both explicit and hidden expenses in digital asset markets.

- *Base Rates:* Borrowing rates typically fluctuate between 7–12% annually. Managers should conduct weekly benchmarking across providers, as strategic volume commitments can often secure discounts of 100–200 basis points.
- *Hidden Fees:* Withdrawal costs, settlement charges, and service add-ons can increase the true cost of capital by 2–4% annually. Automated tracking systems are required to capture these costs, supported by monthly reconciliations of actual versus quoted rates.
- *Collateral Haircuts:* Providers apply "haircuts" that reduce effective collateral value. While BTC and ETH typically receive 60–70% recognition, smaller tokens may receive significantly less or no credit. Weekly monitoring of haircut schedules and automated alerts for changes are mandatory.
- *Opportunity Cost:* Idle collateral in margin accounts represents foregone yield. Managers should use collateral optimization algorithms to minimize idle capital while maintaining sufficient buffers to prevent liquidations.

Financing concentration creates dependency that manifests at the worst time. Relying primarily on a single prime broker or lending source means their problems become yours—and financing providers under stress often reduce exposure precisely when clients need capacity most. The 2022 crypto credit crisis illustrated how quickly financing relationships can unwind. Best practice is maintaining diversified financing relationships even when concentration offers better terms or operational simplicity. For each material financing source, document what happens if the relationship terminates with minimal notice: alternative providers, capacity available, and timeline to transition. Testing backup relationships periodically validates they remain viable.

7.4 LEGAL AGREEMENTS AND DOCUMENTATION

Managing leverage in digital assets requires a clear legal framework that defines the rights and responsibilities of all parties. Agreements establish the ground rules for pledging collateral, custody, and financing terms, while specifying how to resolve disputes or handle defaults during periods of market stress. Each contract must include cryptocurrency-specific provisions to address unique risks—such as 24/7 market operation and blockchain forks—that standard financial templates often overlook.

7.4.1 ESSENTIAL AGREEMENT TYPES

- *ISDA Master Agreement:* Governs OTC derivatives. Standard terms require substantial modifications for digital assets, including expanded collateral definitions (e.g., major tokens with specific haircuts or regulated stablecoins) and 24/7 settlement procedures. Default events must be expanded to include exchange hacks, prolonged network failures, or regulatory prohibitions.
- *Prime Brokerage Agreement:* Defines financing and custody terms. Critical negotiation points include rehypothecation limits (typically capped at 140% of debit balances), clear liquidation methodologies with minimum notice periods, and 24/7 operational support requirements.
- *Credit Support Annex (CSA):* Establishes the collateral framework. Essential provisions include valuation methodologies (using multiple independent pricing sources to avoid oracle manipulation) and clear substitution rights for collateral.
- *Securities Lending Agreement:* Enables borrowing for short positions. Key terms must include recall timing, indemnification for hard forks or airdrops, and rigorous mark-to-market procedures.
- *Custody Agreement:* Governs asset safekeeping. Critical elements include bankruptcy remoteness of client assets, segregation standards (individual vs. omnibus accounts), and explicit liability limits for key loss or theft.

7.4.2 CRYPTOCURRENCY-SPECIFIC PROVISIONS

Agreements must incorporate unique provisions to safeguard assets and ensure proper governance in a decentralized environment:

- *Hard Fork and Airdrop Handling:* Specify who receives the economic benefits from protocol distributions. The baseline standard is that the client is entitled to all distributions from positions held as collateral.

- *Blockchain Network Failures:* Address prolonged congestion, consensus failures, or chain splits. Force majeure clauses must be tailored to these specific operational risks.
- *Stablecoin Considerations:* Define triggers for stablecoin substitution or increased haircuts if a major stablecoin loses its peg.
- *Regulatory Changes:* Include termination rights or mandatory term modifications if local regulations (like the 2026 GENIUS or CLARITY Acts) prohibit specific activities.
- *Key Management:* Explicitly define multi-signature requirements, authorization procedures, and the specific duties of care regarding private key security.

7.4.3 AGREEMENT MANAGEMENT PRACTICES

Legal agreements are living documents that require ongoing management. Investment managers in the digital asset space should regularly review and update these agreements to ensure they remain effective and compliant with current regulations. Proper management helps mitigate risks and supports sound fiduciary practices. It is important to treat these agreements as active tools that need continuous attention to adapt to changing circumstances and maintain their relevance and enforceability.

- *Regular Review:* All agreements should be reviewed quarterly to ensure terms remain appropriate amid market shifts. An annual comprehensive audit with legal counsel is required.
- *Consistency Checking:* Cross-check terms across various counterparties to ensure financing and redemption provisions align. Inconsistent "gates" or collateral terms create operational confusion and legal vulnerability during a crisis.
- *Counterparty Monitoring:* Continuously track the financial condition of counterparties. Deterioration in creditworthiness (e.g., a drop in capital adequacy) should trigger immediate renegotiation or termination discussions.
- *Version Control:* Maintain a centralized archive with full version history, amendment dates, and approvals. This is essential for dispute resolution and passing regulatory examinations.

Institutional investors are increasingly scrutinizing rehypothecation terms following losses from unlimited rehypothecation by firms like Genesis and Celsius. It is important to understand rehypothecation limits, which assets are excluded, and how to monitor counterparty asset usage. Having the right to recall assets is ineffective if the prime broker has already lent them out without restrictions. Investment managers in the digital asset space should review rehypothecation agreements carefully, ensure clear limits are in place, and implement effective monitoring to safeguard assets. Clear policies and regular oversight help mitigate risks associated with rehypothecation practices.

7.5 CRISIS RESPONSE REQUIREMENTS

Leverage and liquidity frameworks are truly tested during rapid market declines. When prime brokers freeze services and investors seek immediate redemptions, digital asset markets react with a velocity that far exceeds traditional finance. In these moments, survival depends on rapid, disciplined decision-making. Managers must prepare for these high-velocity scenarios by establishing rigorous protocols before a crisis occurs.

7.5.1 PRE-CRISIS PREPARATION

Effective crisis management is built during periods of stability. Firms must maintain three specific components ready for immediate activation:

Early Warning System:

Monitoring must trigger alerts based on both absolute thresholds and rate-of-change indicators. While a 20% price drop over 24 hours may be manageable, a 20% drop in 20 minutes requires an entirely different response level. Systems should be configured to flag:

- Leverage utilization approaching house or protocol limits.
- Margin coverage declining below internal safety buffers.
- Liquidity reserves falling below anticipated redemption needs.
- Counterparty stress indicators (e.g., widening CDS spreads or social media sentiment shifts).
- Breakdowns in historical asset correlations.

Decision Authority Matrix:

Clarity of command is essential when seconds count. This document must explicitly define:

- Who can deploy emergency capital and the maximum allowable amounts.
- Who is authorized to approve position liquidations and the associated size limits.
- Designated spokespeople for counterparties, investors, regulators, and the board.
- Specific conditions under which standard operating procedures may be overridden.
- *Note: This matrix should be reviewed quarterly and distributed to all essential personnel.*

Communication Templates:

Crisis updates should be edited, not written from scratch. Pre-drafted templates for various stakeholders (investors, counterparties, regulators) ensure rapid and professional communication.

- *Immediate Awareness (0–2 hours):* Confirms the firm is aware of the event and is monitoring the situation.
- *Initial Detailed Update (2–6 hours):* Provides specific impact assessments and immediate actions taken.
- *Ongoing Status:* Standardized daily updates until the crisis is resolved.

7.5.2 CRISIS RESPONSE PROTOCOL

Firms must establish a phased response workflow with clear decision points:

- *Phase 1: Detection and Assessment (0–30 minutes):* The response team assembles immediately. Documentation begins instantly, recording every data point reviewed and action taken. The focus is on determining current exposure across all venues, identifying liquidity available for mobilization within two hours, and assessing counterparties at risk of immediate failure.
- *Phase 2: Stabilization (30 minutes – 2 hours):* Priority is given to "defensive" actions—posting additional collateral to prevent automatic liquidations, executing hedges to reduce directional bias, and opening lines of communication with critical counterparties to negotiate breathing room.
- *Phase 3: Strategic Response (2–24 hours):* Once immediate threats are contained, the focus shifts to systematic deleveraging, activating backup financing facilities,

and implementing the liquidity "waterfall" if redemptions exceed standard buffers. Material actions at this stage require Investment Committee or Board approval.

Stress tests provide value only when scenarios are severe enough to reveal vulnerabilities. Tests using moderate drawdowns when digital assets have historically experienced 50%+ declines provide limited insight. Effective stress testing requires scenarios that reflect actual historical crises plus plausible future scenarios specific to digital assets. Best practice is maintaining a scenario library that includes: historical replay (March 2020, May 2021, 2022 credit crisis), hypothetical severe scenarios (major exchange failure, stablecoin collapse, regulatory shock), and portfolio-specific scenarios targeting key exposures. Scenario assumptions should be documented and results should inform risk limits, liquidity reserves, and contingency planning.

7.5.3 CRISIS SEVERITY FRAMEWORK

To ensure the response is proportional to the threat, firms categorize incidents using a standardized severity scale:

TABLE 2: CRISIS SEVERITY FRAMEWORK

Level	Severity	Description	Action Required
Level 1	Critical	Systemic failure (e.g., major exchange collapse, 50%+ market crash, smart contract exploit).	Immediate activation of full Crisis Response Team and Board notification.
Level 2	Major	Significant impact on a subset of assets or a single counterparty; 20–30% drawdown.	Activation of stabilization protocols; Head of Risk oversight.
Level 3	Moderate	Noticeable but manageable volatility or minor operational glitches.	Heightened monitoring; standard PM/Ops intervention.

7.5.4 CRISIS TESTING REQUIREMENTS

Documented procedures are only as effective as the results of their most recent test. To maintain institutional-grade readiness, firms must move beyond static plans and implement a rigorous schedule of practical simulations. The goal is to build "muscle memory" within the response team, ensuring that actions are reflexive rather than improvisational during a genuine market event.

Quarterly Unannounced Drills

Firms should execute realistic crisis simulations without advance warning to test actual readiness. These drills should involve waking the response team with a high-impact scenario—for example: "*Major exchange offline, 40% drawdown in Tier 1 assets, and $50M in immediate redemption requests.*" Key performance indicators (KPIs) to measure include:

- *Assembly Time:* How long it takes the Crisis Response Team to convene.
- *Assessment Velocity:* The time required to produce an initial exposure report.
- *Execution Accuracy:* Whether emergency hedges or collateral moves were performed correctly.
- *Note: Any identified failures must be remediated with documented proof within 30 days.*

Annual Comprehensive Exercise

A full-day, multi-factor simulation that tests the firm's entire ecosystem. This exercise should include participation from the Board of Directors for high-level decision-making, rehearsals of investor communications, and coordination with legal counsel for regulatory notification procedures. Engaging external facilitators is recommended to ensure objectivity and to incorporate "black swan" variables that internal teams might overlook.

Tabletop Exercises

Quarterly discussion-based sessions focused on strategic decision-making without full operational execution. These exercises should analyze recent industry failures (e.g., the 2022 credit crisis or 2024–2025 protocol exploits) and evaluate how the firm's current playbooks would have performed. By 2026, best practices for tabletops include simulating AI-powered social engineering attacks or instantaneous stablecoin de-pegging events.

Documentation and Remediation

All testing must be recorded in a formal audit trail to demonstrate compliance with fiduciary standards. Documentation requirements include:

- *Scenario Parameters:* Detailed assumptions, market prices used, and the specific failure mode simulated.
- *Timeline of Events:* A minute-by-minute log of team actions, decisions made, and the rationale for those decisions.
- *Gap Analysis:* Identification of technical bottlenecks, communication silos, or authority ambiguities.
- *Remediation Plan:* Specific action items, assigned owners, and hard deadlines for updating playbooks or technology.

> Risk reporting provides value when it enables decisions, not just documents exposures. Comprehensive reports that bury critical information in detail may obscure rather than illuminate. Effective risk reporting highlights what requires attention: limit utilization approaching thresholds, concentration changes, stress test results, and emerging risks. Best practice is maintaining tiered reporting: an executive dashboard highlighting key metrics and exceptions for senior management and board, with detailed supporting analysis available for those requiring deeper information. Reports should clearly distinguish normal operating conditions from situations requiring escalation or action.

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional allocators assess their risk management by testing how well they handle stress scenarios, diversifying their financing sources, and preparing for crises. If they cannot monitor leverage in real-time, produce liquidity stress test results, or clearly explain how they manage redemptions, it indicates weaknesses in their leverage and liquidity risk management processes.

Leverage Management and Monitoring

- What are your specific leverage limits and current actual usage across all sources including traditional prime brokers and DeFi protocols?

- Walk through your margin management procedures across all venues. Show real-time leverage monitoring dashboard.
- How do you systematically stress test leverage under extreme scenarios?
- What is your worst leverage-related loss and what lessons were learned?

Liquidity Assessment

- Show detailed liquidity tier bucketing analysis with stress test assumptions. Can I see results of your most recent liquidity stress test?
- How do you match assets to investor redemption terms? What is portfolio liquidity under stressed market conditions?
- How do you operationally manage actual redemption requests? Describe liquidation procedures and predetermined waterfalls.
- Have you ever gated investors? Why and how was it managed?

Financing Relationships

- Who are your prime brokers and what active backup relationships exist?
- How do you manage financing costs? What backup financing sources exist if primary relationships fail?
- For DeFi protocols used for financing, how do you evaluate safety? What collateral efficiency exists across different venues?
- Provide sample legal agreements with financing counterparties (appropriately redacted).

Crisis Management and Integration

- Walk through your worst actual crisis in detail. Show comprehensive crisis response framework documentation.
- How quickly can you mobilize emergency liquidity? What are specific escalation triggers and decision authorities?
- How do leverage and liquidity interact in your framework? Show integrated real-time monitoring dashboard.
- What cascade failure risks have you identified and mitigated?

Documentary Evidence Requirements

- Leverage and Liquidity Management Policy
- Current real-time leverage and liquidity reports showing usage against limits

- Stress test results from most recent quarter with scenarios and assumptions
- List of financing counterparties with amounts provided by each
- Prime broker and ISDA agreements (appropriately redacted)
- Crisis response procedures and recent drill results
- Post-mortem reports from material past events
- Live demonstration of real-time integrated monitoring dashboard

---

COMMON PITFALLS AND REMEDIATION

- *Leverage calculation excludes derivatives.* Reported leverage reflects explicit borrowing but ignores futures, perpetual swaps, and options notional—understating true economic exposure by multiples. A fund showing 1.5x leverage may have 5x effective exposure. Remediation: Calculate leverage inclusive of all derivative notional across venues. Report both gross and net exposure. Stress test leverage evolution under adverse scenarios where margin requirements spike and positions must be reduced.
- *Liquidity analysis assumes normal markets.* Portfolio liquidity assessed using average trading volumes and typical bid-ask spreads—conditions that don't hold during stress when liquidity is actually needed. Remediation: Model liquidity under stressed conditions: 50%+ volume reduction, spread widening, exchange withdrawal delays, and correlated selling across venues. Use historical crisis periods (March 2020, May 2022) to calibrate assumptions.
- *Financing concentrated with single provider.* Primary financing relationship provides convenience but creates dependency—counterparty stress becomes your emergency precisely when alternatives are hardest to secure. Remediation: Diversify financing across multiple providers with no single source exceeding 30-40% of capacity. Maintain active backup relationships, not just documented ones. Test backup access periodically to confirm availability.
- *Stress scenarios miss digital asset dynamics.* Stress testing applies generic equity drawdowns rather than crypto-specific events: exchange insolvency, stablecoin depegging, regulatory action, protocol exploit, or cascading DeFi liquidations. Remediation: Develop scenario library reflecting actual digital asset crisis modes. Each scenario should specify assumptions, model portfolio impact, and identify actions that would be triggered. Update scenarios as new risk patterns emerge.

- *Leverage limits exist but aren't enforced*. Limits breached repeatedly with retroactive approval or tacit acceptance. Limits that routinely flex provide no actual constraint. Remediation: Implement hard limits with automated monitoring and immediate escalation. Require written justification and defined remediation timeline for any temporary exception. Track breach frequency—repeated breaches indicate limits miscalibrated or risk culture problems.
- *Counterparty due diligence is superficial or stale*. Financing relationships established based on terms and convenience without credit assessment, or initial diligence never refreshed as counterparty circumstances change. Remediation: Implement formal counterparty framework including initial credit assessment, ongoing monitoring triggers, and annual comprehensive review. Assign internal risk ratings that inform exposure limits.
- *No contingency for financing provider failure*. Assumption that primary relationships will remain available. When a prime broker or lender fails or withdraws, scrambling for alternatives under pressure. Remediation: Document specific alternative providers for each financing source. Maintain active standby relationships—not just identified names but tested access. Know how quickly you could transition and what capacity would be available.
- *Risk dimensions monitored in silos*. Leverage tracked by one system, liquidity by another, counterparty exposure by a third—no integrated view of how risks combine under stress. Remediation: Build consolidated risk dashboard showing leverage, liquidity, and counterparty exposure together. Model how stress scenarios affect all dimensions simultaneously—a liquidity crisis is also a leverage crisis and a counterparty crisis.
- *Agreements treated as static documents*. Financing and counterparty agreements executed and filed without ongoing review. Terms become outdated, unfavorable provisions go unnoticed, renegotiation opportunities missed. Remediation: Review material agreements annually with legal counsel. Track key terms (margin requirements, termination triggers, rehypothecation rights) in accessible format. Renegotiate proactively as relationship value and market conditions evolve.
- *Crisis response untested until actual crisis*. Procedures documented but never drilled. During actual crisis, confusion about roles, communication failures, and delayed decisions determine outcomes. Remediation: Conduct crisis simulation exercises at least annually—unannounced where possible. Test actual decision-making, not just plan review. Document failures identified and remediate before the real event.

KEY CONTROLS AND DOCUMENTATION

Document Type	Purpose	Update Frequency	Ownership
Leverage Policy	Comprehensive leverage limits and procedures	Annual review	CRO/CIO
Liquidity Policy	Complete liquidity management framework	Annual review	CRO/Chief Financial Officer (CFO)
Financing Strategy	Sources diversification and optimization	Quarterly review	CFO
Prime Broker Agreements	Legal contracts defining relationship terms	As needed	Legal/COO
Margin Procedures	Margin management and monitoring protocols	Quarterly review	Operations
Redemption Procedures	Investor liquidity management processes	Semi-annual review	COO/CFO
Crisis Response Plan	Emergency procedures and decision authorities	Quarterly review	CEO/CRO
Stress Test Results	Leverage and liquidity stress testing outcomes	Monthly execution	Risk Management
Financing Cost Analysis	Cost tracking and optimization analysis	Monthly reporting	Finance
Liquidation Playbook	Emergency liquidation waterfall procedures	Quarterly review	CIO/COO
Counterparty Exposure	Financing source concentration monitoring	Weekly review	Risk Management
Daily Liquidity Report	Current liquidity position and coverage	Daily production	Operations
Post-Mortem Reports	Crisis response analysis and improvements	After each crisis event	CRO

STANDARD 8: SAFEKEEPING OF ASSETS

Firms must implement institutional-grade custody. This includes a custody framework with appropriate controls commensurate with assets under management; segregation of client assets from proprietary assets with clear documentation and reconciliation; and multi-layer security architecture including physical security and cybersecurity controls. Firms must maintain comprehensive insurance coverage appropriate to assets under management and custody model and conduct regular security assessments and maintain incident response procedures.

Digital asset custody is quite different from traditional securities custody. Digital assets are controlled by private keys, which act as bearer instruments. Once a transaction is completed, it cannot be reversed. Unlike traditional assets, there is no central authority or clearinghouse to recover lost or stolen assets. If a private key is lost, the asset is permanently gone, even if legal ownership documents exist. Successful hacking incidents can also lead to irreversible losses. Custody failures in digital assets are final; for example, incidents like Mt. Gox and QuadrigaCX resulted in total customer asset losses with limited options for recovery.

Investment managers should use secure and reliable custody solutions for digital assets. The choice of custody depends on the firm's ability to operate and its risk level. It is essential to carefully evaluate third-party custodians, paying attention to their security features and financial health. Adding multiple security layers, such as hardware security modules and multi-signature systems, can improve safety, especially when managing assets in-house. Clear procedures for approving transactions help prevent unauthorized transfers. Good custody practices are based on engineering principles—such as systematic controls, backup safeguards, and ongoing monitoring—rather than just vigilance, ensuring the safety and integrity of digital assets.

Firms can develop a disciplined approach to custody security by treating it as an engineering process. This includes ensuring proper segregation of duties so no single person can authorize transfers alone, keeping detailed logs of all custody activities and access, regularly testing security through penetration tests and audits, and understanding that institutional custody may reduce operational flexibility compared to less secure options.

8.1 CUSTODY MODELS

Digital asset custody operates through three primary models, each presenting distinct advantages, risks, and operational requirements. Model selection depends on firm strategy, risk tolerance, operational capabilities, regulatory requirements, and asset liquidity needs. No single model proves universally optimal—firms often combine multiple approaches creating hybrid architectures matching specific requirements.

TABLE 1: DIGITAL ASSET CUSTODY MODEL

Model	Characteristics, Advantages, and Risks
Self-Custody	Firm directly holds and manages private keys. Provides maximum control, operational flexibility, and eliminates counterparty risk. However, requires sophisticated security infrastructure, experienced personnel, comprehensive insurance, and assumes full responsibility for security. Appropriate for firms with strong technical capabilities and security expertise. Key risks: internal theft, operational errors, inadequate security controls, key loss.
Qualified Custodian	Entrusts private keys to qualified custodian. Transfers security burden to specialized provider with dedicated infrastructure, insurance, and regulatory oversight. Reduces operational complexity and provides institutional credibility. However, introduces counterparty risk, reduces operational control, creates dependency on custodian capabilities. Appropriate for most institutional managers. Key risks: custodian insolvency, security breach, operational failures, limited asset support.
Technology Solution Providers	Uses custody technology providers offering MPC or networked custody. Provides operational efficiency, trading connectivity, broad asset support, and DeFi capabilities. However, regulatory status varies, may include self-custody elements, and insurance structure complexity. Appropriate for active trading strategies and sophisticated operations. Key risks: regulatory uncertainty, technology provider dependency, insurance gaps, security model variations.
Hybrid Custody	Combines self-custody and third-party custody based on asset characteristics and use cases. Typical structure: third-party custody for long-term holdings, self-custody for active trading or DeFi participation. Balances security, flexibility, and operational efficiency. Requires maintaining two custody systems and clear asset allocation

Model	Characteristics, Advantages, and Risks
	policies. Appropriate for sophisticated firms managing diverse strategies. Key risks: complexity, inconsistent security standards, unclear asset segregation.

Custody governance fails when individuals who make investment decisions also control asset movement without independent verification. Effective custody requires segregation between trading authority and custody authorization—no single individual should be able to complete an asset transfer unilaterally, regardless of their seniority or role. Best practice is implementing multi-party authorization for all material asset movements, with authorization requirements documented in custody procedures and enforced through technical controls where possible. The governance framework should clearly specify who can initiate transfers, who must approve, what documentation is required, and what controls prevent circumvention.

8.2 THIRD-PARTY CUSTODIAN DUE DILIGENCE

Investment managers using third-party custodians need to carefully check that these custodians have strong security measures, good operational skills, financial stability, and follow regulations. The quality of custodians can vary a lot—some have top-level security and full insurance, while others may not have enough capital or proper controls. It is important to do a thorough review before choosing a custodian and to keep checking their performance regularly during the relationship.

8.2.1 KEY DUE DILIGENCE AREAS

A comprehensive custodian assessment should cover the following mission-critical operational domains:

- *Regulatory Status and Compliance*: Managers must verify if a custodian is a "qualified custodian" under the Investment Advisers Act or a state/nationally chartered trust company. In the U.S., look for institutions compliant with the 2026 Digital Asset Banking Act and the CLARITY Act, which mandate 1:1 asset reserves and quarterly independent audits.

- *Technology and Security Architecture:* Assess the private key storage technology, favoring Hardware Security Modules (HSMs), Multi-Party Computation (MPC), and geographically distributed Multi-signature arrangements. Review the provider's cold vs. hot wallet allocation policies and verify cybersecurity certifications like SOC 2 Type II or ISO 27001.
- *Insurance Coverage:* Verify policy limits for crime (theft/fraud), cyber (hacking), and specie (physical loss). Adequate insurance should cover a significant portion of the total assets under custody. Investigate the financial ratings of insurance carriers and clarify policy exclusions—such as losses due to protocol-level forks or certain DeFi interactions.
- *Financial Condition and Stability:* Review audited financial statements to ensure capitalization is adequate relative to the AUM. In 2026, regulators often expect Tier 1 capital ranges between $6M and $25M for digital asset trust banks. Assess the sustainability of their business model and the stability of their ownership structure.
- *Governance and Internal Controls:* Evaluate the management team's technical expertise and the independence of the Board. Confirm strict segregation of duties—ensuring no single custodian employee can authorize a transfer—and review transaction approval hierarchies.
- *Operational Capabilities:* Confirm support for required blockchains, tokens, and activities like staking or governance voting. Assess the quality of API integrations, reporting frequency, and the responsiveness of technical support during periods of high market volatility.

8.2.2 ONGOING MONITORING

Due diligence is a continuous process. Ongoing monitoring identifies deteriorating conditions before they result in asset loss:

- *Quarterly Reviews:* Verify updated financial statements, 1:1 reserve attestations, insurance renewals, and operational metrics (e.g., system uptime and error rates).
- *Annual Re-assessment:* Conduct a comprehensive refresh including on-site visits (where practical), reviews of business continuity test results, and deep dives into new security audit findings.
- *Event-Driven Reviews:* Trigger immediate re-evaluations following security "near-misses," regulatory enforcement actions, or significant changes in the custodian's management or ownership.
- *Concentration Monitoring:* Maintain custodian concentration limits to prevent over-reliance on a single provider. Fiduciaries should have contingency plans—

and ideally pre-onboarded secondary custodians—to facilitate rapid asset migration if a primary provider fails.

> Assuming all qualified custodians offer equivalent protection is a common mistake. Insurance coverage, security architecture, financial stability, and regulatory status vary significantly across providers. Marketing claims about "institutional-grade security" require verification through independent due diligence. Best practice is conducting documented custodian due diligence that includes: SOC 2 Type II reports (or equivalent), insurance certificates with coverage details, financial statements or evidence of financial stability, security architecture review, and regulatory status verification. This diligence should be refreshed periodically—custodian circumstances change, and the assessment from two years ago may not reflect current conditions.

8.3 SELF-CUSTODY SECURITY FRAMEWORK

Firms electing for self-custody must implement a comprehensive security framework based on defense-in-depth principles. This ensures that no single failure—whether technical, physical, or human—can result in asset loss. Self-custody security integrates specialized technology with rigorous physical controls and procedural safeguards to create redundant protection against both external hackers and internal collusion.

8.3.1 KEY MANAGEMENT ARCHITECTURE

The architecture design determines the "threshold of failure." A robust setup ensures that multiple independent breaches must occur simultaneously to compromise a private key.

Hardware Security Modules (HSMs):

Fiduciaries should use HSMs for secure key generation and storage. These devices are tamper-resistant and perform all cryptographic operations internally, meaning the private key never touches a network-connected computer.

- *Standard:* Units should be FIPS 140-2 Level 3 (or the newer 140-3) certified, which requires identity-based authentication and physical tamper-response mechanisms that "zeroize" (erase) keys if the device is opened.

- *Deployment:* Best practices include geographic distribution of HSMs and using diverse hardware vendors to mitigate supply-chain vulnerabilities.

Multi-Signature (Multi-Sig) Configurations:

Multi-sig removes "single-key risk" by requiring M-of-N signatures to authorize a move.

- *Operational Wallets (2-of-3):* Provides redundancy while maintaining speed for daily activities.
- *Treasury Wallets (3-of-5*): Increases security by requiring a broader consensus.
- *Cold Storage (4-of-7):* The gold standard for large holdings, maximizing security through geographic and organizational distribution.

Shamir's Secret Sharing (SSS):

SSS is a cryptographic method that "shards" a private key into multiple pieces. Unlike MPC, where the key is never fully formed, SSS temporarily reconstructs the key to perform a signature.

- *Use Case:* Primarily used for secure off-chain backups and disaster recovery.
- *Control:* Reassembled keys must be destroyed immediately after use to prevent "residual" key fragments from remaining in memory.

8.3.2 PHYSICAL AND PROCEDURAL CONTROLS

Technology alone cannot ensure security. It is important to also have physical security measures and clear procedures in place. These help prevent unauthorized access and reduce errors during operations. For digital asset managers, combining technology with physical safeguards and well-defined processes is essential for effective security management.

- *Physical security:* HSMs and backup shards should be stored in high-security facilities like bank vaults or professional safety deposit boxes. Access must be restricted via biometrics and logged with 24/7 video surveillance.
- *Procedural controls:* Written protocols must cover the entire key lifecycle: generation, storage, rotation, and destruction. Procedures should be granular enough for trained personnel to follow without improvisation.
- *Segregation of duties:* Fiduciaries must separate the roles of Key Custodian, Transaction Initiator, and Final Approver. This ensures that unauthorized transfers require a high level of collusion.

- *Background checks:* Comprehensive background checks (criminal, credit, and employment) are mandatory for any staff with custody access, with immediate revocation of privileges upon termination.

Key Generation Ceremonies:

The most critical moment for any self-custody system is the key generation ceremony. This formal procedure ensures the key is secure from the moment of inception:

- *Entropy Verification:* Use multiple independent, "true" random number generators to ensure the key isn't predictable.
- *Witnessing:* Use multiple participants and independent observers to document every step.
- *No-Visibility Rule:* No single individual should ever see the complete seed phrase or private key during the process.
- *Immediate Backup:* Generated keys must be moved into their final secure storage (e.g., SSS shards in bank vaults) immediately following the ceremony.

> Self-custody fails when key management architecture includes single points of failure. A hardware wallet in one location, a seed phrase in one safe, or signing authority concentrated with one person—each creates a vector that must be eliminated for institutional-grade security. Best practice is implementing defense-in-depth: multi-signature or MPC arrangements requiring multiple parties, geographic distribution of key components, and operational procedures ensuring no single person can complete high-value transactions. The architecture should be designed so that multiple independent failures—technical, physical, and human—must occur simultaneously before assets are compromised.

8.4 CUSTODY TIER FRAMEWORK AND GOVERNANCE

Effective custody requires organizing assets into distinct security levels based on their operational utility. This tiered framework balances the need for maximum security with the requirement for immediate liquidity. Strategic holdings are kept in highly restricted environments, while assets for daily operations are managed in more accessible tiers. This approach ensures that protection levels are commensurate with the risk profile and trading frequency of the underlying assets.

8.4.1 CUSTODY TIER STRUCTURE

Firms should allocate assets across four distinct levels, each with specific access controls and security architectures.

Tier 1: Cold Storage (60–80% of Assets)

This tier provides the highest security for long-term strategic holdings.

- *Architecture:* Air-gapped HSMs or qualified custodians using high-threshold multi-signature (e.g., 3-of-5 or 4-of-7).
- *Controls:* Geographic distribution of key holders, storage in bank-grade physical vaults, and a mandatory 24–48 hour delay for withdrawals.
- *Usage:* Strategic reserves and core long-term positions not required for active operations.

Tier 2: Warm Storage (15–30% of Assets)

Warm storage balances institutional security with moderate operational flexibility.

- *Architecture:* MPC or 2-of-3 multi-signature institutional custody.
- *Controls:* Segregated storage with dual-approval requirements and withdrawal whitelisting. Access is typically measured in hours (2–6 hours).
- *Usage:* Operational reserves, funding for active rebalancing, and approved DeFi protocol interactions.

Tier 3: Hot Wallets (5–10% of Assets)

Hot wallets provide maximum flexibility but carry elevated risk due to persistent internet connectivity.

- *Architecture:* Exchange-based accounts or dedicated hot wallet servers with single-signature authority for speed.
- *Controls:* Real-time transaction monitoring, automated reconciliation, and strict programmatic transaction limits.
- *Usage:* Active trading, immediate liquidity needs, and market-making operations.

Tier 4: Protocol Positions (Variable)

This tier encompasses assets deployed directly into smart contracts for yield or utility.

- *Architecture:* Smart contract-controlled assets with protocol-dependent access (e.g., staking or liquidity pools).

- *Controls:* Position-specific risk monitoring and documented "emergency exit" procedures for protocol failures or de-pegging events.
- *Usage:* Staking, lending, and yield optimization strategies.

8.4.2 REBALANCING GOVERNANCE

To maintain the integrity of the tier framework, fiduciaries must implement a disciplined rebalancing process.

- *Threshold Monitoring:* Automated alerts should trigger when the allocation in any tier deviates significantly from policy targets (e.g., a "hot" wallet exceeding 10% of AUM).
- *Sweep Procedures:* Excess funds in Tier 3 should be "swept" to Tier 1 or 2 daily to minimize the potential impact of a hack.
- *Approval Hierarchies:* Moving assets from Cold to Hot tiers must require higher-level executive approval than moving from Hot to Cold, reflecting the increased risk profile.
- *Audit Trails:* Every movement between tiers must be logged with a clear business rationale and verified against the firm's internal ledger.

8.5 SETTLEMENT INFRASTRUCTURE & COLLATERAL MANAGEMENT

Institutional digital asset management requires robust settlement systems that minimize counterparty risk and maximize capital efficiency. In the 2026 landscape, the industry has shifted away from keeping assets on centralized exchanges. Instead, fiduciaries utilize Off-Exchange Settlement (OES) and Tri-Party frameworks that allow for seamless execution while keeping assets under the protection of a regulated custodian.

8.5.1 OFF-EXCHANGE SETTLEMENT FRAMEWORK

Off-exchange settlement minimizes the need to move assets between custody and exchanges, reducing "hot wallet" exposure and simplifying the trade lifecycle.

- *Bilateral Settlement Structures:* Trades occur directly between counterparties, supported by credit relationships rather than pre-funding. Settlement occurs on a T+0 to T+2 basis, with netting agreements significantly reducing transaction volume.

- *Settlement Workflow:* The process moves from trade execution (credit limit verification) to a confirmation phase (blockchain address matching), and finally to the settlement phase where net positions are moved on-chain with cryptographic finality.

8.5.2 TRI-PARTY COLLATERAL MANAGEMENT

Tri-party structures solve the "trust" dilemma in institutional trading by using a neutral third party to manage collateral according to programmatic rules.

- *Tri-Party Custody Model:* A qualified custodian assets for both parties. Trading permissions are granted without moving the assets, allowing for instant, book-entry settlement with maximum regulatory clarity.
- *Network Settlement Model:* Specialized platforms connect counterparties. Assets remain in segregated wallets, and Atomic Swaps ensure "delivery-versus-payment" (DvP), meaning both sides of the trade occur simultaneously or not at all.
- *Smart Contract Escrow:* Collateral is locked in a transparent on-chain contract. This eliminates counterparty credit risk and enables 24/7 automated release logic, though it requires rigorous smart contract auditing.
- *Netting Arrangements:* Bilateral netting aggregates 50+ individual trades into a single net payment. This typically results in an 85%+ reduction in blockchain transactions, providing massive savings on gas fees and reducing operational overhead.

8.5.3 BANKING INFRASTRUCTURE

Traditional banking remains the critical link for cash management and on-ramp/off-ramp activity. Current standards require a Multi-Bank Strategy to ensure redundancy.

- *Redundancy Requirements:* Maintain at least three active banking relationships across different regions.
- *Activity Testing:* Each relationship must process transactions monthly to ensure the rails remain open. Emergency transfer procedures (moving capital between banks) must be tested quarterly.

8.5.4 DIGITAL COLLATERAL MANAGEMENT

The "collateral evolution" has moved basic crypto toward sophisticated, yield-bearing instruments that combine blockchain efficiency with traditional stability.

- *Stablecoin Framework:* Stablecoins (primarily USDC and USDT) are now the primary 24/7 settlement rail for institutional finance.
- *Regulatory Compliance:* Under the 2026 GENIUS Act, fiduciaries should only use stablecoins with 1:1 liquid reserves (Cash/T-bills) and monthly independent attestations.
- *Collateral Utility:* Programmable stablecoins allow for real-time margin adjustments and automated yield-bearing collateral through integration with tokenized money market funds.

TABLE 2: STABLECOIN FRAMEWORK

Stablecoin Type	Primary Use Cases	Risk Factors	Mitigation Strategies
Fiat-Backed (USDC, USDT)	Exchange collateral, trading settlement, liquidity buffer	Issuer risk, redemption delays, and regulatory uncertainty	Diversification across issuers, regular attestation review, redemption testing
Crypto-Collateralized (DAI)	DeFi operations, protocol integration, yield generation	Collateral volatility, protocol risk, governance changes	Monitoring collateralization, protocol diversification, governance participation
Algorithmic	Unsuitable for institutional use due to stability concerns and historical failures		

Tokenized Securities as Collateral:

Tokenized treasuries and money market funds (MMFs) represent a transformative shift in digital asset management. These instruments combine the high credit quality and legal stability of traditional government-backed securities with the 24/7 programmable efficiency of blockchain technology. This allows managers to utilize yield-bearing instruments as collateral, optimizing capital efficiency while maintaining a conservative risk profile.

- *Key Features:* Products are typically SEC-registered with daily Net Asset Value (NAV) calculations and are 1:1 backed by government securities or repurchase agreements.
- *Primary Benefits:* Tokenized securities provide institutional-grade regulatory clarity and established oversight. They generate yield while simultaneously serving as collateral for trading and are available for atomic settlement 24/7, bypassing traditional banking hours.
- *Implementation Considerations:* Managers should prioritize SEC-registered products with proven track records. It is essential to maintain diversification across multiple issuers and platforms to prevent concentration risk. Managers must also verify that their selected execution venues or prime brokers accept these specific tokenized instruments for margin purposes.

8.5.5 ACCOUNT CONTROL AGREEMENTS

Account Control Agreements (ACAs) are essential legal instruments in digital asset lending and prime brokerage. They allow a secured party (lender) to "perfect" their security interest in digital assets held by a third-party custodian without requiring the physical transfer of those assets to the lender's own wallet. This "tri-party" framework provides a secure and efficient way to manage collateralized loans and margin trading.

ACA Framework Requirements:

- *Real-Time Enforcement:* The custodian must possess the technical capability to enforce control instructions within minutes. The system must be able to block transfers or freeze accounts instantly without further borrower approval once a "Notice of Exclusive Control" is triggered.
- *Legal Perfection:* Managers must obtain legal opinions confirming the perfection of the security interest under relevant laws, such as UCC Article 12 (governing Controllable Electronic Records) which gained widespread adoption by 2026.
- *Technical Integration:* The custodian's API must integrate directly with the lender's risk management systems to support automated margin calls and liquidation procedures.

Critical Capabilities:

- *Response Speed:* Maximum response time for control instructions must be documented in a Service Level Agreement (SLA), typically requiring action within 15 minutes.

- *Granular Controls:* The infrastructure should support partial restrictions or "springing" controls rather than simple all-or-nothing account blocks, allowing for more nuanced risk management.

8.6 INSURANCE AND RISK TRANSFER

Comprehensive insurance provides a critical layer of protection against custody-related losses and enables the transfer of risk to traditional carriers with robust capital reserves. Today, the digital asset insurance market has matured, but remains complex due to varying exclusions and specific "security warranties" that can void a policy if not strictly followed.

8.6.1 CUSTODIAN INSURANCE EVALUATION

Most institutional custodians include insurance as a core component of their service offering. However, the quality and breadth of protection differ significantly between providers. Investment managers must conduct a granular analysis of these programs to ensure that coverage aligns with the fund's risk profile and asset allocation.

Coverage Structure Assessment

The most critical distinction in an insurance program is between dedicated and shared coverage:

- *Dedicated Coverage:* Provides specific policy limits for a single client, ensuring clear claim priority and preventing the "first-come, first-served" exhaustion of funds.
- *Shared Coverage:* Pools limits across the custodian's entire client base. In the event of a platform-wide breach, allocation formulas may leave individual funds with inadequate recovery.
- *Verification Requirements:* Managers should obtain insurance certificates, policy declarations specifying the structure (dedicated vs. shared), and financial strength ratings (e.g., A.M. Best or S&P) for the underlying carriers.

Coverage Scope Analysis

Actual protection is often dictated by the specific "wallet tier" where assets reside:

- *Cold Storage:* Typically receives the most comprehensive coverage with the lowest deductibles due to its offline nature.

- *Hot & Warm Storage:* Coverage is often severely limited or excluded entirely for internet-connected wallets, despite these tiers carrying the highest operational risk.
- *DeFi & Staking:* Standard custody policies frequently exclude assets deployed in smart contracts or staking protocols.
- *Verification Requirements:* Review the complete policy wording, including asset coverage lists (specifying supported blockchains/tokens) and exclusion schedules to identify protection gaps.

Exclusions and Warranties

Policy "fine print" can render insurance void if specific conditions are not met.

- *Common Exclusions:* Many policies do not cover social engineering (even if MFA was bypassed), losses from "authorized-but-fraudulent" transactions, or vulnerabilities in third-party smart contracts.
- *Security Warranties:* These are contractual requirements the manager or custodian must follow to maintain coverage. Common warranties include mandatory use of FIPS-certified HSMs, specific multi-signature thresholds, and strict incident notification timeframes.
- *Verification Requirements:* Documentation must show that current operational procedures (e.g., 3-of-5 multi-sig) match the warranties specified in the insurance contract.

Claims Process Requirements

A policy is only valuable if it pays out efficiently during a crisis. Managers should evaluate the following:

- *Notification Windows:* Procedures often require formal notice within 24–72 hours of a suspected incident.
- *Submission Standards:* Requirements for forensic analysis, security logs, and transaction records needed to substantiate a claim.
- *Track Record:* Research the carrier's historical claims experience and average settlement timeframes within the digital asset sector.

8.6.2 CUSTODIAN INSURANCE LANDSCAPE

The digital asset insurance market is segmented by provider type, each offering different levels of protection and operational trade-offs. Institutional managers must match their specific

strategy—whether long-term holding or active DeFi participation—to the appropriate insurance profile.

- *Qualified Custodians:* These providers typically offer dedicated "crime and specie" policies with clear limits and bankruptcy protection. They provide client-specific certificates and align with the 2026 CLARITY Act standards. However, they often exclude hot wallets and offer minimal protection for assets deployed in staking or DeFi protocols.
- *Technology Platforms:* These entities utilize shared coverage pools that include Technology Errors and Omissions (E&O) components. This provides better coverage for API-driven transactions and broader asset support. It should be noted that shared limits across the entire client base can lead to "limit exhaustion" during systemic events, and claims procedures are often technically complex.
- *Exchange Custodians:* Often feature exchange-wide policies with massive aggregate limits, providing a seamless experience for high-frequency traders. However, assets are frequently commingled, and coverage may be tied to the exchange's overall solvency rather than specific client accounts, creating significant bankruptcy risk.
- *Bank Custodians:* Banks leverage traditional, multi-billion-dollar financial institution policies with extensive E&O coverage and balance-sheet protection. However, they are often restricted to "blue-chip" assets (BTC, ETH) and require highly restrictive security models that can hinder operational speed.

Insurance evaluation helps managers distinguish between those with a deep understanding of coverage and those who see it as just a basic service. When reviewing insurance programs, evaluators should ask for clear and complete documentation. This includes insurance certificates from custodians showing coverage limits and insurance providers, detailed policy wording with any exclusions clearly marked, and proof of additional coverage policies. It is also important to perform a gap analysis to identify uncovered risks and understand how they are managed. Additionally, a claims process framework should be reviewed to ensure proper handling of claims. During due diligence, key questions should be addressed: What happens if a custodian experiences a security breach? Can you walk through the claims process step by step? What are the notice requirements for filing claims? Who is responsible for submitting claims? What portion of assets is covered by dedicated insurance versus shared coverage? Where are the coverage gaps, and what measures are in place to address them? Vague statements about having "comprehensive insurance" without supporting documentation often indicate a lack of understanding of insurance coverage. Clear, detailed documentation and a thorough review process are essential for effective risk management in digital asset investments.

8.7 MULTI-CUSTODIAN ARCHITECTURE AND SELECTION

Concentration risk in digital asset custody represents an existential threat to fund operations. Unlike traditional finance, where sub-custody is an invisible operational layer, the "bearer instrument" nature of digital assets means that a single provider failure can lead to total, irreversible loss. Today, institutional policies increasingly mandate a Multi-Custodian Architecture. This approach moves beyond simple safekeeping, treating custody as a strategic resilience layer that prevents single points of failure, mitigates jurisdictional risk, and ensures 24/7 market access.

8.7.1 CUSTODIAN SELECTION FRAMEWORK

Selecting the right mix of custodians involves matching specific operational needs—such as trading frequency and asset diversity—with the appropriate regulatory and security profile.

Primary Decision Factors:

- *Regulatory Requirements:* Qualified custodian status mandatory for regulated fund vehicles, more flexibility for separately managed accounts, institutional allocators typically expect qualified custody. Consider jurisdiction-specific rules and investor requirements.
- *Trading Activity Level:* High-frequency trading requires custody with exchange connectivity and APIs, daily/weekly rebalancing needs warm wallet capabilities, monthly-plus rebalancing emphasizes cold storage with scheduled access.
- *Asset Diversity:* Bitcoin/Ethereum only provides widest custodian options, mid-cap assets require verification of specific token support, DeFi participation needs MPC with protocol connectivity, staking requirements need specialized support.
- *Risk Tolerance:* Conservative approach emphasizes qualified custodians with bankruptcy-remote structures, balanced approach combines qualified custody with technology platforms, progressive approach accepts more self-custody with sophisticated controls.

TABLE 3: CUSTODIAN PROVIDER COMPARISON

Provider Type	Primary Strengths	Key Limitations	Best Use Cases
Bank Custodians	Regulatory clarity, balance sheet strength, institutional reputation	Limited asset coverage, slower innovation, higher costs	Regulated funds, conservative allocators, traditional institutions
Qualified Crypto Custodians	Regulatory status, crypto expertise, broader asset support	Higher costs, operational constraints, variable insurance	Regulated vehicles, institutional mandates, compliance-first approach
Technology Platforms	Operational efficiency, trading integration, DeFi connectivity	Regulatory questions, self-custody elements, insurance complexity	Active strategies, trading operations, DeFi participation

Provider Type	Primary Strengths	Key Limitations	Best Use Cases
Self-Custody Solutions	Maximum control, no counterparty risk, cost efficiency	Operational burden, key management risk, insurance challenges	Experienced teams, technical expertise, specialized strategies

8.7.2 DUE DILIGENCE FRAMEWORK

A thorough evaluation of custodians involves a systematic review of various aspects to ensure reliability and efficiency. This process helps investment managers, especially those handling digital assets, to select the most suitable custodians for their needs. Key areas of assessment include security measures, compliance with regulations, operational capabilities, technological infrastructure, and customer support.

By carefully analyzing these factors, digital asset managers can make informed decisions, reducing risks and enhancing the safety of their investments. This standardized approach ensures consistency and thoroughness in evaluating custodians, which is essential for maintaining trust and integrity in digital asset management.

- *Regulatory Assessment:* Qualified custodian status under Investment Advisers Act or equivalent. Licenses in all operating jurisdictions with capital adequacy. Regulatory examination history and outstanding actions. Legal opinions confirming bankruptcy-remote structure. AML/KYC procedures and sanctions screening capabilities.
- *Operational Evaluation:* Uptime history targeting 99.9%+ availability with downtime documentation. Asset coverage breadth across blockchains and token types. Integration capabilities through APIs and technical documentation. Transaction processing capacity and scaling plans. Reporting quality, frequency, and customization options. Customer support responsiveness and technical expertise.
- *Financial Analysis:* Balance sheet strength with capital adequacy relative to custody assets. Audited financial statements showing profitability trends. Funding sources and runway adequacy (minimum 18 months). Credit ratings if available from recognized agencies. Ownership structure stability and shareholder quality. Business model sustainability and revenue concentration analysis.

- *Technical Architecture:* Security architecture including HSMs, multi-signature, MPC implementation. Key management procedures and geographic distribution. Cold versus hot storage allocation policies. Third-party security audits and penetration testing results. Incident history including breaches, near-misses, and responses. Cybersecurity certifications (SOC 2 Type II, ISO 27001). Business continuity and disaster recovery with tested procedures.
- *Governance and Controls:* Board composition with independent directors and relevant expertise. Management team experience in both traditional finance and digital assets. Internal control framework with SOC 2 Type II attestation. Segregation of duties in custody operations. Transaction authorization procedures preventing single-person control. Audit committee oversight with external audit reports.

Red Flags: Lack of a 1:1 reserve attestation, pending regulatory enforcement, vague security descriptions, or "shared" insurance limits that could be exhausted by other clients.

8.7.3 MULTI-CUSTODIAN ALLOCATION

Using different types of custodians helps lower risk by avoiding over-reliance on a single provider. It also improves the overall management of digital assets. Diversification is no longer optional; it is a baseline requirement for institutional resilience.

- *Allocation Review:* Conduct quarterly re-assessments of each custodian's risk profile. If a provider's financial health or regulatory status changes, an immediate rebalancing evaluation is required.
- *Contingency Planning:* Maintain "warm" backup relationships with secondary custodians. This includes having legal agreements and API integrations pre-configured.
- *Migration Testing:* Periodically rehearse asset migration procedures (e.g., a "paper exercise" or small-scale transfer) to estimate the time required for an emergency exit—typically targeting a 1–2 week window for full migration in a crisis.

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional allocators assess custody by examining the security measures, settlement processes, insurance coverage, and how custodians are chosen. If they cannot show strong security controls, provide complete insurance documents, or clearly explain settlement procedures, it indicates weaknesses in custody practices.

Custody Model and Architecture

- What is your custody model and why did you choose it? Describe your custody architecture including key management and security layers.
- If you use third-party custodians, provide your due diligence report evaluating their capabilities, financial condition, insurance coverage, and security controls.
- If you self-custody, walk through your key management architecture including multi-signature arrangements, hardware security modules, and access controls.
- Show your custody tier framework with allocation targets and actual allocations. When did you last rebalance?

Settlement Infrastructure

- How do you handle off-exchange settlement? What bilateral and tri-party arrangements exist?
- Walk through a complete settlement workflow from execution through post-settlement reconciliation.
- What netting arrangements exist with counterparties? Show settlement documentation.
- Describe your banking infrastructure. How many banking relationships do you maintain and why?
- How do you utilize stablecoins and tokenized securities as collateral?
- Do you have Account Control Agreements in place? How do they function operationally?

Security Controls and Authorization

- Walk through your transaction authorization process. Who can initiate, approve, and execute asset movements?
- What security audits have been completed? Provide results of most recent penetration test and SOC 2 audit.

- How do you protect private keys and prevent unauthorized access? Show key management procedures.
- Have you had any security incidents in the past two years? If so, how did you respond?
- Can the CEO override transaction approvals? Walk through the override process if it exists.

Insurance and Risk Transfer

- What insurance coverage do you maintain? Provide complete insurance certificates showing limits and carriers.
- Is custodian insurance dedicated or shared? What is the claims process?
- What supplemental insurance do you carry directly? Show gap analysis identifying uncovered risks.
- Provide your insurance coordination document showing how multiple policies respond.
- Walk through a hypothetical custody loss scenario. Which insurance responds and what is the recovery process?

Multi-Custodian Architecture

- How many custodians do you use and what is the allocation across them?
- Walk through your custodian selection process. Show due diligence reports on current custodians.
- What concentration limits exist preventing over-reliance on single custodian?
- How quickly could you migrate to backup custodian if primary relationship failed?
- Show recent custodian review documentation with quarterly monitoring.

Operational Controls

- How do you authorize large transfers? Walk through a $10M withdrawal from cold storage.
- What are your reconciliation procedures and frequency? Provide sample daily reconciliation report.
- Show your wallet inventory with all addresses and purposes.
- What counterparty concentration limits exist for settlement?
- How do you manage collateral optimization across venues and counterparties?

Documentary Evidence Requirements

- Custody Policy with security controls, tier framework, and authorization procedures
- Third-party custodian due diligence reports with annual updates
- Self-custody key management architecture diagrams (if applicable)
- SOC 2 Type II reports from all custodians
- Recent penetration test and security audit results
- Settlement agreements and bilateral credit arrangements
- Credit Support Annex (CSA) documentation with collateral schedules
- Account Control Agreements for prime brokerage (if applicable)
- Insurance policies and certificates showing coverage (custodian and direct)
- Insurance coordination document and gap analysis
- Custodian selection documentation including RFP and evaluation
- Multi-custodian allocation policy with concentration limits
- Daily custody reconciliation reports with break resolution documentation
- Incident response logs and resolution documentation
- Key generation ceremony documentation (if applicable)
- Wallet inventory with addresses, purposes, and authorization levels
- Transaction authorization logs showing approval workflows
- Board minutes approving custody arrangements

COMMON PITFALLS & REMEDIATION

- *Custodian selected without rigorous due diligence*. Custodian chosen based on reputation or convenience without assessing financial strength, security architecture, insurance coverage, regulatory status, or operational controls. Marketing claims accepted without verification. Remediation: Implement comprehensive due diligence covering: SOC 2 Type II reports, insurance certificates with coverage details, financial statements, security architecture

review, and regulatory standing. Document findings and reassess annually—custodian circumstances change.

- *Multi-signature is nominal, not real.* Multi-sig wallet exists but one person controls multiple keys, or keys are stored together, or approval can be bypassed through management override. The control exists on paper only. Remediation: Ensure genuine key independence: different individuals, different locations, different organizational reporting lines. Test periodically by confirming no single person or location compromise could authorize transactions. Document key holder roles and geographic distribution.
- *Hot wallet balances exceed operational needs.* Convenience drives holding large balances in internet-connected wallets, creating unnecessary exposure to compromise. A single security failure can result in material loss. Remediation: Limit hot wallet holdings to operational minimums—typically under 5% of assets. Implement automated sweeps to cold storage when balances exceed thresholds. Monitor hot wallet activity daily with alerts for unusual patterns.
- *Senior executives can override custody controls.* CEO or CIO can bypass approval requirements citing urgency or authority. Override capability negates the control structure entirely—if one person can move assets unilaterally, multi-sig provides no protection. Remediation: Eliminate override authority completely, regardless of seniority or circumstances. Every transaction follows standard approval workflow. Document this explicitly in custody policy and test that technical controls enforce it.
- *Security assessments infrequent or absent.* Penetration testing and security audits performed once at launch or never. Vulnerabilities accumulate undetected as systems evolve and threat landscape changes. Remediation: Conduct penetration testing at least annually and after significant infrastructure changes. Require SOC 2 Type II audits for any custody operations. Track findings to remediation with defined timelines.
- *Incident response undocumented or untested.* No defined procedures for security breach, or procedures exist but have never been exercised. During actual incident, confusion about roles and communication delays worsen outcomes. Remediation: Document incident response covering: detection and classification, escalation matrix, communication protocols, containment procedures, and recovery steps. Conduct tabletop exercises at least annually. Update procedures based on exercise findings.
- *Physical security neglected.* Focus on cybersecurity while physical protection of key material, hardware wallets, and seed phrase backups receives inadequate attention. Physical compromise can bypass all technical controls. Remediation:

Implement physical security for all key material: restricted access, surveillance, tamper-evident storage, and environmental controls. Distribute backups geographically. Include physical security in periodic security assessments.

- *Key recovery procedures untested*. Recovery process documented but never executed. Assumptions about access, timing, and coordination unvalidated until actual emergency—when discovering problems is too late. Remediation: Test key recovery procedures at least annually under realistic conditions. Simulate various scenarios: key holder unavailable, hardware failure, facility inaccessible. Document test results and remediate gaps immediately.
- *Third-party custodian oversight lapses after onboarding*. Initial due diligence performed but ongoing monitoring neglected. Custodian control environment may deteriorate without detection. Remediation: Require annual SOC report review and attestation updates from custodians. Monitor for regulatory actions, security incidents, or material changes. Maintain escalation procedures for identified deficiencies—and willingness to transition if issues aren't resolved.
- *Insurance coverage assumed adequate without analysis*. Reliance on custodian's insurance without understanding coverage limits, exclusions, deductibles, or claim procedures. Gaps discovered only when filing a claim. Remediation: Obtain and review custodian insurance policies—not just certificates. Conduct gap analysis against actual risk exposures. Consider supplemental direct coverage for gaps. Document coverage coordination and test claims process understanding.
- *Assets concentrated with single custodian*. Majority of holdings with one provider regardless of quality—creating single point of failure if custodian experiences security breach, insolvency, or operational failure. Remediation: Implement multi-custodian architecture with concentration limits (30-40% maximum per custodian). Maintain backup custodian relationships with tested onboarding. Document migration procedures for rapid transition if needed.

KEY CONTROLS & DOCUMENTATION

Document	Purpose	Update Frequency	Owner
Custody Policy	Comprehensive custody framework	Annual	COO

Document	Purpose	Update Frequency	Owner
Settlement Procedures	Off-exchange settlement protocols	Quarterly	Operations
Collateral Management Policy	Collateral posting and optimization	Semi-annual	Risk/Ops
Security Procedures	Detailed security protocols	Quarterly	CTO
CSA Documentation	Credit support agreements	As needed	Legal
Key Management Policy	Key generation, storage, usage	Semi-annual	Security
Custodian Agreements	Legal contracts with custodians	As needed	Legal
Settlement Agreements	Bilateral trading agreements	As needed	Legal
Insurance Policies	Coverage documentation	Annual	CFO
Access Control Matrix	Who can access what	Monthly	COO/CTO
Wallet Inventory	All wallets and purposes	Weekly	Operations
Counterparty Limits	Settlement and credit limits	Monthly	Risk
Incident Response Plan	Security incident procedures	Semi-annual	CTO
Audit Reports	Security and operational audits	Annual	External

STANDARD 9: COUNTERPARTY MANAGEMENT

Firms must manage counterparty risk. This includes thorough due diligence processes for all counterparties and service providers before engagement; diversification across trading venues and counterparty relationships to reduce concentration risk; and ongoing monitoring of counterparty creditworthiness and operational risk. Firms must document contingency plans for counterparty failures or service disruptions and conduct regular assessment of service provider performance and capabilities.

Counterparty risk in digital assets encompasses operational and technological failures that extend far beyond traditional credit risk. Many exchanges and service providers operate with varying levels of transparency, leaving them vulnerable to insolvency or internal mismanagement. The 2022 collapse of FTX remains a landmark case study, demonstrating the dangers of over-reliance on a few dominant entities; such failures can lead to immediate capital loss and years of complex bankruptcy proceedings for exposed firms. Because the digital asset ecosystem is highly interconnected, a single counterparty default can trigger a chain reaction, impacting custodians, prime brokers, and market makers simultaneously.

Standard 9 mandates a disciplined, proactive approach to managing these exposures. For institutional managers today, this involves a "defense-in-depth" strategy: conducting rigorous initial due diligence, enforcing strict exposure limits, and maintaining continuous monitoring. Stability can shift rapidly in digital markets; therefore, assessments must move beyond static annual reviews toward real-time risk tracking. This ensures that a counterparty's financial health and security posture are verified against the firm's specific risk tolerances on an ongoing basis.

Managing counterparty risk is a dynamic process that requires accepting certain trade-offs. To protect client assets, managers must prioritize diversification—spreading exposure across multiple venues and jurisdictions—even if this increases operational costs or reduces execution speed. Effective oversight includes regular "on-site" or virtual audits, tracking aggregate exposure across all relationships, and utilizing third-party blockchain analytics to monitor counterparty wallet health. Institutional-grade management values long-term stability and capital preservation over the convenience of concentrated relationships or lower trading fees.

9.1 COUNTERPARTY RISK MANAGEMENT FRAMEWORK

Rigorous due diligence on all counterparties is the cornerstone of risk management. Initial assessments must be comprehensive, while ongoing reviews ensure that the counterparty's financial and operational health remains within acceptable thresholds. This process should move beyond surface-level reviews to include deep-dive assessments of technical, financial, and regulatory maturity.

9.1.1 COUNTERPARTY UNIVERSE AND TIERING

Defining the counterparty universe establishes a complete view of all entities creating risk. In digital asset markets, this universe typically includes:

- *Exchanges:* Centralized venues (e.g., Coinbase, Kraken, Binance) and decentralized exchanges (DEXs). Centralized venues present custodial risk, while decentralized venues present smart contract risk.
- *Prime Brokers:* Entities providing financing, custody, and execution. These relationships often create concentrated exposure requiring rigorous oversight.
- *OTC Desks:* Market makers for bilateral trading. Risks include settlement lag during execution and credit risk if trading on margin.
- *Custodians:* Third-party entities holding firm assets. These represent the largest single counterparty exposures and require the most stringent monitoring.
- *Lending Protocols:* DeFi platforms for borrowing or lending. Risks include smart contract vulnerabilities, governance failures, and oracle manipulation.
- *Service Providers:* Administrators, auditors, and technology vendors. While not direct financial counterparties, operational dependencies create significant secondary risks.

Counterparty Tiering

Firms should classify entities based on exposure size and operational criticality to determine monitoring frequency:

- *Tier 1 (Critical):* Largest exposures or essential infrastructure. Requires comprehensive oversight, including annual on-site visits and quarterly monitoring updates.
- *Tier 2 (Important):* Material exposure or specialized services. Requires semi-annual reviews.

- *Tier 3 (Routine):* Limited exposure or infrequent usage. Requires annual documentation refreshes.

9.1.2 COUNTERPARTY RISK LIMITS

Specific, measurable limits for each counterparty and the aggregate portfolio are essential to prevent dangerous concentration.

Individual Counterparty Limits: Maximum exposure to a single entity, often expressed as a percentage of Net Asset Value (NAV). Typical institutional ranges include:

- Tier 1 Custodians: 40–50% (dependent on bankruptcy-remote status).
- Exchanges: 10–20%.
- OTC Desks: 5–10%.

Aggregate Limits: Total exposure across categories to prevent sector-wide failure impact. This includes caps on total exchange exposure or total exposure to unregulated entities.

Exposure Measurement: A standardized methodology must calculate total exposure, including:

- Assets held by the counterparty.
- Financing/leverage provided.
- Unsettled transactions and margin requirements.
- Potential Future Exposure (PFE) from derivatives.

Limit Monitoring: Daily calculation of current exposure versus limits. Automated alerts should trigger when approaching thresholds, and all breaches must be documented with a clear remediation timeline.

> Counterparty due diligence performed at onboarding and never revisited loses value over time. Exchange solvency, protocol security, and lending platform stability change continuously. The counterparty approved 18 months ago may have materially different risk characteristics today.Best practice is establishing a periodic review cycle for all material counterparties, with review frequency based on exposure size and counterparty risk characteristics. Reviews should assess current financial condition, operational changes, regulatory developments, and any incidents since the last review. Documented procedures ensure reviews happen systematically rather than only when problems emerge.

9.2 COUNTERPARTY DUE DILIGENCE

Effective counterparty risk management begins with disciplined, risk-based due diligence. Comprehensive review of a counterparty's financial condition, governance, risk management framework, and operational resilience is essential to informed exposure decisions. Diligence standards should increase proportionately with counterparty tier and exposure size, requiring deeper verification for Tier 1 and Tier 2 relationships.

9.2.1 DUE DILIGENCE FRAMEWORK

A comprehensive due diligence framework systematically examines the critical domains of a counterparty's business. This standardized approach allows managers to identify hidden vulnerabilities and ensures that all partners meet the minimum safety requirements for institutional capital.

TABLE 1: COMPREHENSIVE ASSESSMENT FRAMEWORK

Assessment Category	Investigation Areas	Verification Methods	Critical Red Flags
Corporate Structure	Legal entity mapping, Ownership transparency, Jurisdictional analysis	Entity searches, Ownership checks, Legal opinions	Opaque structures, Offshore-only, Anonymous ownership
Financial Health	Audited statements, Proof of reserves, Revenue sources, Capital adequacy	Independent audits, On-chain testing, Stress testing	Missing audits, Unverified reserves, Undercapitalized
Operational Capability	Technology infrastructure, Security measures, Settlement reliability	Architecture review, Penetration testing, Settlement testing	Frequent outages, Breach history, Settlement delays
Regulatory Compliance	Licensing status, Compliance program, Regulatory actions	Database checks, Framework review, Public records	No licenses, Regulatory actions, Weak compliance
Management Quality	Executive backgrounds, Track record, Governance structure	Background checks, Reference calls, Organizational assessment	Anonymous management, Past failures, Founder dependency

Detailed Due Diligence Pillars

- *Business and Reputation*: Beyond basic history, this involves reviewing the business model's sustainability and client concentration. Background checks on key executives are mandatory to identify legal issues or prior failures that could indicate future governance risks.
- *Financial Condition:* Fiduciaries must analyze capitalization adequacy relative to the counterparty's operational risk. This includes assessing liquidity positions, funding sources, and Proof of Solvency—the verification that on-chain assets exceed customer liabilities.
- *Regulatory and Legal:* Verification of registration with relevant authorities and the "bankruptcy-remoteness" of client assets is essential. This ensures that in the event of insolvency, the fund's assets are not treated as part of the counterparty's general estate.
- *Risk Management:* Evaluation of internal governance, including limits on their own market and credit risk. This pillar also covers the adequacy of their insurance program and the results of recent disaster recovery testing.
- *Technology and Security:* Focuses on the security of the custody stack and key management systems. It requires proof of recognized certifications such as SOC 2 Type II or ISO 27001, alongside a review of system uptime and API scalability.

9.2.2 ON-SITE VISITS AND ONGOING MONITORING

On-site visits (or "virtual deep-dives" using live screen-sharing for tech audits) are vital for Tier 1 counterparties. Firsthand interaction with senior management allows for a better assessment of their capabilities, while observing operational controls can reveal the reality of their organizational culture. Observing facility security and interacting with compliance teams provides insights that static documentation cannot capture.

Due diligence is a continuous obligation. Monitoring frequency is strictly tied to the counterparty's tier:

- *Tier 1 (Critical):* Quarterly monitoring updates of financial statements and operational metrics. Requires an annual comprehensive re-assessment including a site visit.
- *Tier 2 (Important):* Semi-annual monitoring reviews with a full due diligence refresh every year. Site visits are conducted every 2–3 years or upon a "trigger" event.

- *Tier 3 (Routine):* Annual monitoring review with a refresh of due diligence documents every 2–3 years. On-site visits are only conducted if material concerns are identified.

> Exchange selection based primarily on liquidity and fees, without assessment of financial stability and asset protection practices, proved costly during the 2022 exchange failures. Proof of reserves claims, regulatory status, insurance coverage, and asset segregation practices warrant independent verification rather than reliance on marketing materials. Best practice is maintaining documented due diligence files for material exchange relationships that include: proof of reserves verification (methodology and limitations), regulatory licenses and status, published insurance coverage, and analysis of asset segregation practices. Exposure limits should reflect assessed counterparty quality, with lower limits for exchanges where verification is limited.

9.3 EXCHANGE MANAGEMENT

Exchanges are a vital component of the digital asset market infrastructure, yet they represent a significant concentration of counterparty risk. Unlike traditional finance, where trading venues and custodians are strictly separated, many digital asset exchanges operate as "all-in-one" platforms. This dual role creates an environment where an exchange failure—as demonstrated by the 2022 collapse of FTX—can lead to the immediate loss of all assets held on that platform and result in years of complex, uncertain bankruptcy litigation. Managing this risk requires a disciplined approach to exchange selection, rigorous exposure limits, and active monitoring of withdrawal functionality.

9.3.1 EXCHANGE SELECTION AND MONITORING

A formal approval process is required before trading on any venue to ensure the platform meets institutional safety standards. Investment managers should perform a comprehensive evaluation across several critical domains:

- *Trading Volume and Liquidity:* Analyze the average daily volume (ADV) and order book depth for the specific assets being traded. High headline volume can be misleading; fiduciaries must verify liquidity stability during periods of extreme market stress.

- *Security and Custody:* Evaluate the exchange's custody architecture (e.g., percentage of assets in cold storage) and historical security track record. The availability of regular Proof of Reserves or independent attestations is a primary indicator of transparency.
- *Regulatory Status:* Verify licenses and registrations in all relevant jurisdictions (e.g., U.S. BitLicense or European MiCA-compliant status). Compliance with AML/KYC requirements and the clarity of legal protections in the exchange's Terms of Service are essential.
- *Financial Condition:* Assess the sustainability of the exchange's business model and the quality of its financial backing. Transparency regarding proprietary trading activities or affiliated market makers is critical to identifying potential conflicts of interest.
- *Operational Capabilities:* Monitor system uptime history and API reliability. The exchange must demonstrate high-capacity transaction processing and responsive technical support for institutional clients.

9.3.2 EXPOSURE MANAGEMENT

Active management of exchange balances is the most effective defense against platform failure. Spreading risk across multiple venues ensures that no single collapse can jeopardize the entire portfolio.

Minimize Exchange Balances: Firms should treat exchanges as "trading venues" rather than "storage venues." Excess balances should be "swept" back to cold or warm custody daily or whenever they exceed a defined threshold.

- *Target:* Combined exchange exposure should typically remain under 10% of NAV.
- *Limit:* No single exchange should hold more than 5% of NAV at any given time.

Diversification of Venues: Trading activity must be distributed across a minimum of 3–5 approved exchanges. This prevents dependency on a single provider and ensures that if one venue experiences downtime or a security event, the firm can continue to execute its strategy on alternative platforms.

Withdrawal Testing: Operational readiness is verified through regular withdrawal tests. Managers should perform small, automated withdrawals monthly and larger, manual withdrawals quarterly. Any delay, restriction, or "system maintenance" that impacts withdrawal functionality must be immediately escalated as a high-priority risk event.

Real-Time Monitoring and Alerts: Firms should implement real-time balance tracking with automated alerts for any unusual exchange activity. Daily reconciliations between exchange reporting and internal ledgers are mandatory to ensure that the firm's view of its assets matches the exchange's records.

9.4 LEGAL AND CONTRACTUAL PROTECTIONS

Robust legal agreements are a critical tool for mitigating counterparty risk by clearly defining rights, obligations, and remedies. Given the unique technological nature of digital assets and the evolving regulatory landscape should be negotiated with specialized legal counsel rather than accepting standardized "terms of service."

9.4.1 KEY CONTRACTUAL PROVISIONS

Important parts of a contract include key terms and conditions that must be agreed upon by all parties involved. These provisions ensure that the rights and responsibilities of each party are clear and legally binding.

- *Collateral Requirements:* Agreements must specify the types of digital assets accepted as collateral (e.g., BTC, ETH, or regulated stablecoins like USDC). Crucially, they should define valuation methodologies using multiple independent pricing sources to avoid "oracle" manipulation, and set clear haircuts (valuation discounts) based on asset volatility.
- *Events of Default:* Beyond traditional insolvency, digital asset defaults should include specific technical and regulatory triggers. These may include exchange hacks, prolonged blockchain network failures, or regulatory actions that prohibit the counterparty from handling specific digital commodities.
- *Termination and Liquidation Rights:* Contracts must establish the right to terminate and liquidate collateral immediately upon default. This includes defining the "grace period" for margin calls—which is typically much shorter in digital markets (minutes to hours) than in traditional finance.
- *Asset Segregation and Bankruptcy Remoteness:* A primary goal is ensuring client assets are held in segregated accounts and are legally isolated from the counterparty's general estate. This "bankruptcy-remote" status prevents clients from being treated as unsecured creditors if the counterparty fails.
- *Governing Law and Jurisdiction:* Managers must specify the governing law (e.g., New York or English law) and the jurisdiction for dispute resolution. This is vital

for cross-border transactions where legal treatment of "controllable electronic records" can vary significantly.

9.4.2 NETTING AND SET-OFF

Where feasible, agreements should include netting and set-off provisions to reduce gross counterparty exposure. These provisions are essential for capital efficiency and risk reduction in high-volume trading environments.

- *Bilateral Netting:* Allows a firm to offset its obligations across multiple products and transactions with a single counterparty, resulting in a single "net" exposure.
- *Close-Out Netting:* Upon a default event, this enables the firm to terminate all outstanding trades and offset gains against losses to determine a single net payment amount. This significantly reduces the risk of "cherry-picking" by a bankruptcy trustee.
- *Set-Off Rights:* These provisions allow the firm to apply any collateral or other obligations against amounts owed by the defaulting counterparty, further mitigating potential losses.
- Note: Netting enforceability varies by jurisdiction. Legal counsel must verify that netting provisions are upheld under local insolvency laws, as some regions do not honor these clauses without specific structural documentation.

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional allocators evaluate counterparty management through diversification discipline, exposure monitoring rigor, and contingency planning adequacy. Inability to demonstrate systematic due diligence, produce real-time exposure monitoring, or explain counterparty failure response procedures reveals inadequate counterparty risk management.

Counterparty Framework and Due Diligence

- Walk through your counterparty risk management framework including classification system and tier assignment criteria.
- What is your process for conducting due diligence on new counterparties? Provide sample due diligence report for key counterparty.
- How do you determine and enforce exposure limits across different counterparty types?

- What operational testing protocols apply before allocating to new counterparties?
- Show real-time monitoring systems and alert escalation procedures.

Exchange and Prime Broker Management

- What is your current exposure to your top five counterparties? How do you mitigate risks of holding assets on exchanges?
- Walk through withdrawal testing protocols including frequency and documentation. What tier classification methodology applies?
- Explain multi-prime architecture and activity allocation. How do you prevent concentration creep?
- Show historical decisions where you reduced or eliminated exchange or prime broker relationships.
- Walk through primary counterparty failure response procedures.

Banking and Settlement Risk

- How do you manage bilateral settlement risk across OTC relationships?
- What banking redundancy exists with geographic distribution? How many active banking relationships do you maintain?
- What triggers banking relationship changes or terminations?
- How are 90-day operating expenses distributed across banks?

Documentary Evidence Requirements

- Counterparty Risk Management Policy
- Sample due diligence reports for key counterparties
- Comprehensive counterparty exposure reports with limits and utilization
- Operational testing documentation with withdrawal success rates
- Real-time monitoring dashboards displaying health metrics
- Sample legal agreements with key counterparties
- Performance scorecards and relationship review documentation
- Banking relationship matrix showing institutions, jurisdictions, and balances
- Counterparty failure scenario response procedures

COMMON PITFALLS AND REMEDIATION

- *Counterparty exposure concentrated for convenience*. Majority of trading, custody, or financing through single provider because it's operationally simpler. Concentration risk unrecognized until counterparty failure makes it unavoidable—as FTX demonstrated definitively. Remediation: Enforce diversification limits: no single exchange exceeding 20-30% of trading volume, no single custodian exceeding 30-40% of assets. Maintain active backup relationships, not just identified alternatives. Test contingency access before it's needed.
- *Due diligence performed once and filed*. Counterparty assessed at onboarding but never revisited. Financial condition, control environment, and regulatory status change—the counterparty approved two years ago may have materially different risk characteristics today. Remediation: Implement tiered ongoing monitoring: annual comprehensive review for material counterparties, trigger-based review for adverse events (regulatory action, security incident, key personnel departure). Update risk ratings based on findings.
- *Excessive balances left on exchanges*. Assets remain on exchanges beyond immediate trading needs for convenience, creating uncompensated counterparty exposure. Exchange balances are unsecured creditor claims in insolvency. Remediation: Implement daily sweeps to custody, keeping exchange exposure below 10% of NAV or immediate trading requirements. Conduct periodic withdrawal tests confirming ability to move assets promptly—exchanges that delay withdrawals warrant reduced exposure.
- *Due diligence relies on counterparty representations*. Risk assessment based on what counterparties claim about themselves—proof of reserves, security practices, regulatory status—without independent verification. Self-reported information proved unreliable repeatedly in 2022. Remediation: Verify key claims independently: regulatory licenses through regulator databases, proof of reserves through on-chain verification where possible, security practices through SOC reports or audit attestations. For material relationships, consider on-site visits.
- *Exposure limits breached without consequence*. Limits exist but breaches routinely accepted with informal approval or after-the-fact ratification. Limits that flex on demand provide no actual risk control. Remediation: Implement automated monitoring with immediate alerts at threshold levels (e.g., 80% of limit). Require written justification and senior approval for any breach. Track breach frequency

and duration—repeated breaches indicate limits miscalibrated or trading behavior that needs correction.

- *Standard counterparty agreements accepted without negotiation.* Exchange and custodian terms signed as presented without legal review. Unfavorable provisions—broad rehypothecation rights, weak segregation, disadvantageous default terms—discovered only during counterparty stress. Remediation: Engage counsel experienced in digital asset agreements to review material relationships. Negotiate key terms: asset segregation, rehypothecation limitations, termination rights, and recovery priority. Document negotiation outcomes and accepted residual risks.
- *No contingency plan for counterparty failure.* Assumption that key counterparties will remain operational. When failure occurs, scrambling for alternatives under time pressure and market stress. Remediation: Document contingency plans for each material counterparty: pre-identified alternatives, estimated transition timeline, required actions, and communication protocols. Test plans periodically—a contingency that hasn't been exercised may not work when needed.
- *Counterparty exposure tracked in silos.* Trading desk tracks exchange exposure, treasury tracks banking relationships, operations tracks custody—no aggregated view of total counterparty risk across the firm. Concentration discovered only after problems emerge. Remediation: Centralize counterparty exposure in unified dashboard covering trading, custody, financing, and banking relationships. Implement automated alerts when aggregate exposure approaches limits. Review consolidated exposure regularly at risk committee level.

KEY CONTROLS AND DOCUMENTATION

Document Type	Purpose	Update Frequency	Ownership
Counterparty Policy	Selection, approval, monitoring framework	Annual	Chief Risk Officer

Document Type	Purpose	Update Frequency	Ownership
Approved Counterparty List	Authorized counterparties with tiers and limits	Monthly	Risk Committee
Due Diligence Files	Complete diligence documentation	Initial + Annual refresh	Compliance
Service Agreements	Executed contracts with terms	As needed	Legal Counsel
Exposure Reports	Current exposure by counterparty	Real-time, Daily formal	Operations
Monitoring Dashboard	Real-time health and performance	Continuous	Risk/Operations
Incident Log	Issues, resolutions, lessons learned	Ongoing	Operations
Contingency Plans	Backup arrangements and transitions	Quarterly review, Annual testing	Chief Operating Officer

STANDARD 10: VALUATION AND PERFORMANCE

Firms must establish sound valuation practices. This includes documented valuation policies with independent oversight and regular committee review; multiple pricing sources with defined hierarchy and validation procedures; and valuation committee with regular review of pricing methodologies and fair value determinations. Firms must calculate performance following industry standards appropriate to strategy and reporting frequency and implement quality control procedures for valuation and performance reporting.

Valuing digital assets presents unique challenges, including fragmented liquidity, early-stage illiquid tokens, and complex DeFi products that lack traditional pricing methods. It is common to observe price variances exceeding 5–10% for the identical asset across different exchanges, particularly during periods of market stress. Assets such as illiquid tokens and venture investments often lack observable market prices, necessitating subjective valuation methods that can be vulnerable to manipulation. Furthermore, DeFi instruments—including staked tokens, liquidity pool (LP) tokens, and governance rights—require specialized valuation techniques that have no direct equivalent in traditional finance.

Standard 10 mandates that firms implement robust valuation practices supported by independent oversight and clear performance measurement. This involves establishing comprehensive valuation policies, approved by the board and reviewed annually, and appointing independent Valuation Committees that operate without influence from portfolio managers. Systematic valuation methodologies must be documented for all asset types—with a focus on illiquid holdings—and verified by qualified fund administrators to determine accurate Net Asset Value (NAV).

To meet this standard, firms should separate valuation decisions from investment management, implement quality controls to detect pricing errors, hold regular Valuation Committee meetings to review all complex assets with documented reasons, keep detailed records of all pricing decisions for future review, and accept that conservative valuations might lower reported returns but help maintain investor trust. Allowing portfolio managers to set their own asset values without independent checks can compromise valuation integrity and disqualify firms from attracting institutional investors, regardless of investment success.

10.1 VALUATION FRAMEWORK

The formal valuation framework offers a clear and consistent method for valuing all assets in a portfolio. It prioritizes independence, objectivity, and verifiability over operational ease or favorable results. This framework is the definitive mechanism for determining whether the Net Asset Value (NAV) accurately reflects the true market value of the portfolio or merely represents the portfolio manager's subjective opinion.

10.1.1 VALUATION POLICY

The valuation policy, approved by the board and reviewed each year, should clearly outline the procedures and standards for valuing digital assets. It is essential that the policy is straightforward and easy to understand, ensuring that investment managers can consistently apply valuation methods. The policy should include key elements such as the scope of assets covered, valuation techniques, frequency of reviews, roles and responsibilities, and compliance requirements. Simplifying the language helps ensure clarity and facilitates adherence across the organization, especially for digital asset managers who need precise and accessible guidance for their valuation processes.

Valuation Hierarchy: Assets are categorized into a three-level hierarchy based on the observability of their inputs, aligned with institutional accounting standards (such as ASC 820).

- *Level 1:* Assets with unadjusted quoted prices in active markets (e.g., BTC, ETH on major liquid exchanges).
- *Level 2:* Assets with observable inputs other than quoted prices (e.g., tokens with similar characteristics, or those priced via observable dealer quotes).
- *Level 3:* Assets with unobservable inputs requiring significant judgment (e.g., early-stage venture tokens, certain NFTs, or illiquid DeFi positions). These require the highest level of scrutiny due to valuation subjectivity.

Valuation Sources: Data sources must follow a documented order of preference to prevent "cherry-picking" or selecting sources that favor specific results.

- *Primary:* Independent pricing services or high-volume, liquid exchanges.
- *Secondary/Tertiary:* Backup data aggregators or reputable over-the-counter (OTC) desk quotes used only when primary sources are unavailable.
- *Quality Reviews:* Systematic reviews of these sources must be conducted regularly to identify data gaps or manipulation risks.

Valuation Methodologies: Methodologies must be documented in sufficient detail to allow an independent third party to replicate the valuation.

- *Consistency:* Methods must be applied consistently across reporting periods; any change in methodology requires detailed justification and approval.
- *DeFi Specifics:* Methodologies for liquidity pool (LP) tokens must account for underlying asset values and accrued fees, while staked positions must consider potential slashing penalties and lock-up periods.

Pricing Challenges and Escalation:

Firms must establish clear triggers for investigating pricing issues, such as:

- Stale prices (no update within a defined timeframe).
- Source discrepancies (e.g., a >5% variance between two approved exchanges).
- Material position changes without corresponding price movements.
- Resolution: Documented escalation steps ensure these challenges reach the Valuation Committee for final determination.

> Valuation integrity requires predetermined pricing hierarchies applied consistently. Without clear rules specifying which price source takes precedence, valuations may be selected—consciously or not—in ways that favor performance presentation. This risk is heightened in digital assets where the same token often trades at different prices across venues. Best practice is establishing a documented pricing hierarchy by asset type, specifying primary and secondary sources, and defining procedures for situations where sources conflict or are unavailable. The policy should be applied consistently, with any deviations documented and approved through the valuation governance process.

10.1.2 VALUATION COMMITTEE

The Valuation Committee must be an independent group responsible for overseeing the valuation process. It should be led by a CFO or a senior executive who is not involved in portfolio management. The committee should include a CFO or equivalent financial officer, a Chief Risk Officer or risk management representative, an independent director or board member, and an external valuation expert for complex portfolios. Portfolio managers can

attend meetings to provide background information but should not have voting rights on valuations. The main duties of the committee include:

- Reviewing and approving valuation policy annually
- Approving valuation methodologies for new asset types
- Reviewing all Level 3 asset valuations quarterly minimum
- Investigating and resolving pricing challenges
- Approving manual pricing overrides with documented rationale
- Meeting minutes documenting all decisions and rationale

> Valuation governance requires independence from investment decision-making. The portfolio manager who selected an illiquid position has inherent interest in its valuation. Effective governance interposes independent review—through a valuation committee, administrator authority, or both—between investment professionals and final valuations. Best practice is establishing a valuation committee (or clear administrator authority) with documented responsibility for: approving valuation policies, reviewing complex or illiquid asset valuations, resolving pricing disputes, and overseeing valuation process integrity. Committee composition should include at least one member independent of the investment function.

10.2 VALUATION OF DIGITAL ASSETS

Digital asset valuation requires nuanced approach accounting for each asset's unique characteristics. Valuation methodology appropriateness depends on liquidity, trading venue availability, position size relative to market, and information availability.

TABLE 1: ASSET VALUATION LEVELS

Level	Asset Types	Valuation Methodology
Level 1: Liquid Assets	BTC, ETH, major stablecoins, large-	Use quoted prices from approved exchanges or pricing services. Specify primary source with fallback hierarchy. Volume-weighted average

Level	Asset Types	Valuation Methodology
	cap tokens with deep liquidity	across multiple venues if appropriate. Daily pricing standard.
Level 2: Less Liquid Assets	Mid-cap altcoins, DeFi tokens, assets with inconsistent liquidity	Multiple exchange pricing with volume weighting, third-party pricing services, matrix pricing using comparable assets. Adjustments for position size relative to market liquidity. Staleness checks identifying inactive pricing.
Level 3: Illiquid Assets	Early-stage tokens, venture positions, NFTs, locked/vesting tokens, LP tokens	Discounted cash flow analysis, comparable company/transaction analysis, recent transaction prices with adjustments for time and conditions. Illiquidity discounts applied. Valuation Committee approval required for all Level 3 assets.

10.2.1 LIQUID ASSETS (LEVEL 1)

Liquid assets such as Bitcoin, Ethereum, and major stablecoins are valued using quoted prices from "principal markets"—venues with the greatest volume and level of activity for the asset.

- *Approved Exchange Hierarchy:* The Valuation Policy must maintain a ranked list of approved exchanges (e.g., Coinbase, Kraken, Binancel) based on 24-hour trading volume, regulatory standing, and order book depth.
- *Pricing Aggregation:* Primary pricing should come from independent services (e.g., Coin Metrics or Kaiko) that utilize volume-weighted averaging (VWAP) across multiple venues to mitigate the risk of price manipulation on a single exchange.
- *Frequency and Latency:* Prices are typically updated daily at a standardized "cut-off" time. Backup procedures must be documented for instances where the primary pricing service or principal exchange is unavailable.
- *Quality Controls:* Automated checks must trigger if a price deviates by a defined threshold (e.g., >3%) from the 24-hour average or if data becomes "stale" (no update for >60 minutes).

10.2.2 LESS LIQUID ASSETS (LEVEL 2)

Assets that are less liquid might not have clear, single-market prices. Instead, their value often needs to be estimated using several different data points. This can make valuation more complex and less precise, requiring careful analysis by investment managers.

- *Matrix Pricing:* For tokens that trade infrequently, value may be derived by observing prices of similar "comparable" assets and adjusting for differences in market cap, sector, or utility.
- *Third-Party Validation:* Independent pricing vendors provide "evaluated prices" by aggregating data from thin order books and OTC (Over-the-Counter) desk quotes.
- *Liquidity Adjustments:* If a position represents a significant portion of the total circulating supply, a discount may be applied to reflect the "price impact" of a potential liquidation. These adjustments must be based on empirical analysis of order book depth.

10.2.3 ILLIQUID AND HARD-TO-VALUE ASSETS (LEVEL 3)

Illiquid assets—including early-stage venture tokens, NFTs, and locked/vested positions—require the highest level of judgment. All Level 3 valuations must be approved by the Valuation Committee and documented with a detailed rationale.

Discounted Cash Flow (DCF) Analysis: Used for protocols or tokens with identifiable revenue streams (e.g., transaction fees, staking commissions).

- *Inputs:* Projections of user adoption, protocol growth rates, and terminal value.
- *Risk-Adjusted Rate:* Use a discount rate that reflects the specific technological and regulatory risks of the project.
- *Sensitivity Analysis:* Must be conducted to show how changes in key assumptions (e.g., a 10% drop in user growth) impact the final valuation.

Comparable Company/Transaction Analysis: Valuation is derived using multiples (e.g., Price-to-Total-Value-Locked or Price-to-Earnings) from similar projects or recent private funding rounds. Multiples are adjusted for the project's stage, team quality, and competitive positioning.

Recent Transaction Prices: The "price of recent investment" is often the most reliable input for early-stage assets, provided the transaction was at arm's length.

- *Time Decay:* Adjustments must be made if significant time has elapsed or if market conditions for the specific sector have shifted.

- *Discounts for Lack of Marketability (DLOM):* For tokens subject to vesting or lock-up periods, a discount for lack of marketability must be applied. Common models include the Chaffe or Finnerty models to quantify the cost of being unable to sell the asset during the restriction period.

Valuation Documentation Requirements

To meet institutional and audit standards (such as ASU 2023-08), all Level 3 valuations must include:

- *Methodology Rationale:* Why the specific model was chosen.
- *Supportable Assumptions:* Data-backed evidence for growth rates or multiples.
- *Sensitivity Table:* A range of values based on varying "bull" and "bear" case scenarios.
- *Committee Minutes:* Formal record of the Valuation Committee's approval and any dissenting views.

Complex asset valuation using models or estimates requires documentation sufficient for independent replication and validation. A model producing reasonable outputs today may be miscalibrated in ways that only surface during market stress. Models should have documented assumptions, defined data inputs, and periodic validation against market transactions where possible. Best practice is maintaining written methodology for each valuation model, including: inputs and data sources, key assumptions and their rationale, sensitivity to key variables, and comparison to observable transactions when available. Periodic independent review—whether internal or external—validates that models remain appropriate as market conditions evolve.

10.2.4 ASSET-SPECIFIC METHODOLOGIES

Valuation for DeFi positions requires specialized techniques that go beyond simple market-price aggregation. Because these assets are often "composite" in nature, the valuation framework must account for the underlying collateral, accrued yields, and technical risks unique to smart contract environments.

Liquidity Pool (LP) Token Valuation: LP tokens represent a pro-rata share of a decentralized exchange pool. Their value is non-linear and must be calculated using a "look-through" approach:

- *Net Asset Value (NAV) of Components:* Separately price each underlying asset (e.g., the ETH and USDC in an ETH/USDC pool) using approved Level 1 sources.
- *Accrued Fees:* Include all trading fees earned by the pool that have not yet been "reinvested" into the LP token's value.
- *Impermanent Loss (IL) Adjustment:* Valuation must reflect the current state of the pool's constant product formula (x times y = k). Managers should use the standard IL formula to compare the current LP value against a "buy-and-hold" equivalent to verify the position's performance.

$$IL = \left(2\sqrt{PriceRatio}\right) / \ (1 + PriceRatio) - 1$$

- *Verification:* Cross-reference on-chain data with third-party DeFi aggregators to ensure the smart contract's reported "Total Value Locked" (TVL) aligns with market pricing.

Staking Position Valuation: Staking involves locking native tokens to secure a network in exchange for rewards. The valuation must reflect both the principal and the "work-in-progress" earnings:

- *Principal + Accrued Rewards:* Combine the market value of the base tokens with all rewards earned to date, even if they remain in a "pending" or "unclaimed" state.
- *Lock-up & Illiquidity Discounts:* For tokens in an "unbonding" or fixed-term lock-up period, a discount should be applied to reflect the inability to liquidate the position during market volatility.
- *Slashing Risk:* Valuation should include a "slashing reserve" or risk adjustment if the chosen validator has a history of downtime or if the network's protocol-level penalties are significant.
- *Exit Queue Documentation:* The estimated timeframe for withdrawals (the "unbonding period") must be updated and documented monthly.

Yield Farming Position Valuation: Yield farming often involves multiple layers of rewards, including governance tokens and "boosted" incentives:

- *Daily Reward Tracking:* Track the fair market value of all reward tokens at the time they become "claimable" according to the protocol's smart contract logic.
- *Net Yield Calculation:* Subtract expected transaction costs, such as "gas" fees required to harvest rewards, from the gross yield to determine the net return.
- *APY Verification:* Do not rely solely on the platform's "headline" APY. Managers must independently verify the Annual Percentage Yield by analyzing the rate of reward emissions against the total pool liquidity.

TABLE 2: DISTRESSED ASSET VALUATION (ILLUSTRATION)

Asset Status	Initial Approach	Discount Range	Review Frequency
Exchange Halted/Delisted	Last reliable trade price	20-50% initial discount	Weekly impairment testing
Locked under 30 days	Market price if liquid exists	5-10% illiquidity discount	Review upon unlock
Locked 30-90 days	Market price if liquid exists	10-20% illiquidity discount	Monthly reassessment
Locked 90-365 days	Market price if liquid exists	20-40% illiquidity discount	Monthly reassessment
Locked over 365 days	Market price if liquid exists	40%+ illiquidity discount	Quarterly reassessment
Failed Protocol	Recovery value assessment	50-100% impairment	Bi-weekly monitoring
Litigation/Claims	Probability-weighted outcomes	Case-specific analysis	Per legal development

10.3 PRICING SOURCES AND DATA MANAGEMENT

10.3.1 DATA INFRASTRUCTURE

Pricing data for digital assets originates from a fragmented ecosystem where reliability varies significantly. Exchange APIs are prone to intermittent failures, data providers employ diverse aggregation methodologies, and blockchain explorers may present conflicting on-chain information. Consequently, a robust data management system must ingest data from multiple

independent sources, verify its accuracy in real time, and maintain a comprehensive audit trail of all modifications.

The core challenge lies in balancing automation with human oversight. While manual pricing is operationally unscalable and prone to bias, fully automated systems without validation logic can propagate erroneous data into Net Asset Value (NAV) calculations. An institutional-grade system automates routine pricing tasks but utilizes "exception-based" logic to flag unusual data for manual review by a valuation expert.

10.3.2 PRICING SOURCE ARCHITECTURE

A tiered architecture ensures that the firm is never reliant on a single point of failure for its valuation needs.

TABLE 3. MULTI-TIER SOURCE FRAMEWORK

Source Tier	Primary Use Case	Selection Criteria
Primary Sources	Daily NAV calculation, Official reporting	Institutional grade credibility, Broad asset coverage, Transparent methodology, Regulatory acceptance
Validation Sources	Cross-validation, Discrepancy resolution	Real-time data availability, Granular price detail, API reliability, Independent methodology
Backup Sources	Emergency pricing, Illiquid asset valuation	Always available regardless of market conditions, Decentralized infrastructure, Independent from primary sources

To ensure global comparability and consistency, Coordinated Universal Time (UTC) midnight is the industry standard reference time for daily valuations. Since digital asset markets operate 24/7, this fixed reference point allows administrators to reconcile data across different funds and ensures that market comparisons remain valid.

10.3.3 DATA VALIDATION FRAMEWORK

The validation framework utilizes a layered approach, combining automated tolerance monitoring with manual investigation to ensure data integrity.

Automated Tolerance Monitoring: The system should automatically generate alerts or halt the NAV process if the following thresholds are breached:

- Volatility Spikes: Day-over-day price changes exceeding 10%.

- Source Variance: Price deviations exceeding 5% between primary and validation sources.
- Volume Anomalies: Trading volume falling below 50% of the recent moving average.
- Liquidity Stress: Bid-ask spreads widening beyond 2x normal levels.
- Staleness: Prices remaining unchanged for over 24 hours.

Cross-Validation Procedures: When an automated alert is triggered, the following investigative steps are required:

- Systematically compare primary source data against validation and backup sources.
- Verify "on-chain" data (e.g., DEX pool ratios) for blockchain-native assets.
- Conduct order book analysis to confirm actual market depth at the reported price.
- Contact OTC counterparties directly if material discrepancies arise in high-value positions.

Exception Resolution: All pricing exceptions must be resolved through a documented governance process. This includes a full investigative analysis for every exception and supervisor approval for any manual price overrides. Significant uncertainties or systemic issues must be escalated to the Valuation Committee, with all decisions stored in a permanent audit trail to ensure accountability and transparency for auditors and investors.

> In managing digital assets, it is important not to rely on a single pricing source. Use multiple sources to ensure accuracy: the primary source provides the initial price, the secondary confirms it, and the tertiary resolves any discrepancies. Clearly document your hierarchy of sources and the rules for switching between them. When questioned by auditors, demonstrate a structured approach rather than making arbitrary choices. Proper documentation of your procedures helps protect against claims of manipulation, even if prices change later.

10.4 FUND ADMINISTRATION AND NAV OVERSIGHT

10.4.1 THE NAV PROCESS

Calculating the Net Asset Value (NAV) for digital asset portfolios requires robust, repeatable processes that account for the unique characteristics of the asset class. Unlike traditional funds that typically calculate NAV once daily at a market close, cryptocurrency funds must often produce calculations multiple times per day during periods of extreme volatility.

The accuracy and auditability of the NAV are complicated by several factors:

- *Continuous Accruals*: Real-time staking rewards and yield farming incentives must be accounted for accurately.
- *DeFi Complexity:* Administrators must be able to decompose complex decentralized finance positions into their underlying components for valuation.
- *System Limitations:* Variations in calculation logic or data source integration between the manager and the administrator can lead to discrepancies.

Effective oversight requires a framework that ensures accuracy through rigorous reconciliation while respecting the necessary independence of the third-party administrator.

10.4.2 SHADOW NAV FRAMEWORK

A Shadow NAV process is the primary mechanism for verifying administrator accuracy. It involves the firm's internal finance or risk team performing a parallel NAV calculation using identical position and pricing data to serve as an independent check.

Shadow NAV Components:

- *Tolerance Thresholds:* Discrepancy limits are typically set at 10 basis points (0.10%). Any variance exceeding this threshold triggers a mandatory investigation.
- *Daily Variance Analysis:* Tracking patterns in discrepancies to identify whether errors are systematic (process-driven) or random.
- *Root Cause Investigation:* Determining the specific source of the mismatch to ensure the correct "official" NAV is struck.
- *Documentation Standards:* Maintaining a clear audit trail of all findings, investigations, and final resolutions for review by external auditors.

Common Sources of Discrepancy: To resolve variances effectively, the firm must categorize and address the following common mismatch drivers:

- Pricing source differences: Administrator and manager use different data providers with varying methodologies
- Timing mismatches: Snapshot captured at slightly different times creating legitimate price differences
- Fee accrual variations: Different methodologies for calculating daily management fee accruals
- Corporate action handling: Different treatment of forks, airdrops, or staking rewards
- Foreign exchange rates: Different sources for fiat currency conversion rates

> Fund administrators provide value through independent verification of NAV and other calculations. This independence is compromised when managers influence valuations, pressure timing, or select administrators based on flexibility rather than capability. The administrator relationship should involve appropriate professional tension—administrators should push back when they disagree. Best practice is establishing clear boundaries in the administrator relationship: the administrator controls final NAV calculation within agreed policies, valuation disputes are resolved through documented procedures, and the manager provides information (not direction) for administrator calculations. A relationship where the administrator always defers to manager preferences may not provide the independent verification investors expect.

10.5 PERFORMANCE MEASUREMENT

Accurate performance measurement is essential for evaluating the effectiveness of the investment process and communicating results to investors. Since performance returns are derived directly from the Net Asset Value (NAV), any valuation errors propagate into performance misstatements, potentially leading to investor misinformation.

10.5.1 PERFORMANCE CALCULATION

A clear and well-documented policy for calculating performance is essential. It should specify the methods used, data sources, and calculation procedures. This ensures transparency and consistency in performance measurement, which is crucial for digital asset managers in the investment industry. A straightforward policy helps all stakeholders understand how performance is assessed and reported, fostering trust and compliance with industry standards.

- Calculation methodology: Time-Weighted Returns (TWR): Preferred for liquid strategies to eliminate the impact of external cash flows (contributions and withdrawals), reflecting the manager's skill in asset selection. Money-Weighted Returns (MWR): Used for less liquid or venture-style funds where the manager has significant control over the timing of capital calls and distributions.
- *Fee treatment:* Returns should be presented on both a Gross-of-fee (to show investment skill) and Net-of-fee (to show actual investor experience) basis. Policies must specify the timing of management and performance fee accruals.
- *Benchmark selection: Benchmarks* must be "fit for purpose." For a Bitcoin-only fund, a BTC spot price index is appropriate. For a multi-token DeFi fund, a customized or broad-market index (e.g., the Bloomberg Galaxy Crypto Index) should be used and documented.

10.5.2 PERFORMANCE ATTRIBUTION

Performance attribution identifies the specific sources of returns, distinguishing between intentional strategy and market chance.

- *Allocation Effect:* Returns generated by weighting specific sectors (e.g., Layer 1s vs. DeFi protocols) differently than the benchmark.
- *Selection Effect:* Excess returns generated by picking specific high-performing tokens within those sectors.
- *Interaction Effect:* The combined impact of allocation and selection decisions.
- *Additional Drivers:* Identifying the impact of staking yields, gas costs, leverage, and cash drag on the total return.

10.6 PERFORMANCE REPORTING AND GIPS

The Global Investment Performance Standards (GIPS) are voluntary, ethical guidelines for reporting investment results. Following GIPS ensures that reports are transparent, consistent, and prevent "cherry-picking" of successful periods. Many institutional allocators now require GIPS compliance as a prerequisite for investment.

10.6.1 GIPS COMPLIANCE

GIPS compliance process can be complex and time-consuming but demonstrates commitment to performance reporting standards. Compliance requires: establishing compliant policies and procedures, calculating performance according to GIPS standards, creating composite structures grouping similar strategies, annual verification by independent GIPS verifier, updating disclosures meeting GIPS requirements. Firms pursuing GIPS compliance should engage experienced consultants ensuring proper implementation avoiding common pitfalls.

10.6.2 GIPS VERIFICATION

GIPS verification involves a thorough review by independent, qualified verification firms. This process ensures that digital asset managers follow industry standards and best practices. Verification helps build trust with clients and regulators by confirming that the firm's reporting and procedures are accurate and compliant with GIPS guidelines. It is an essential step for firms managing digital assets to demonstrate transparency and credibility in their operations.

Firm-Wide Verification

- Policies and procedures review ensuring documented processes exist
- Composite construction methodology validation confirming appropriate grouping
- Performance calculation process testing verifying mathematical accuracy
- Presentation standards adherence checking required disclosures
- Disclosure completeness assessment ensuring transparency

Performance Examination

- Provides deeper validation of specific composites beyond firm-wide review
- Tests return calculations at granular security level
- Confirms asset valuations through independent price verification
- Validates all disclosures against supporting documentation

- Offers more detailed assurance than general verification

Verification firms are typically large accounting companies, such as the Big Four, that have expertise in GIPS standards, or specialized verification companies that are qualified to perform these checks. Conducting an annual verification is the basic requirement to stay compliant with GIPS. It is also recommended to review the performance of investment composites used in marketing materials regularly to ensure accuracy and compliance.

10.6.3 GIPS PRESENTATION REQUIREMENTS

GIPS presentation standards help investment managers communicate performance clearly and fairly. These rules make it easier to compare different managers and prevent misleading reports that highlight only good results. Digital asset managers face special challenges in following these standards. For example, tokens often have short price histories, markets operate 24/7 without traditional trading hours, custody arrangements are complex, and prices can be very volatile. These factors require adjustments to the usual presentation formats. The table below explains the main presentation elements and how they should be applied to digital asset portfolios, ensuring transparency and consistency in reporting performance.

TABLE 4: CORE PRESENTATION ELEMENTS

Required Element	Standard Requirement	Digital Asset Adaptation
Performance Table	Minimum 5 years of annual returns, Benchmark comparison	Account for tokens that did not exist historically, Address 24/7 trading versus traditional market hours
Composite Assets	Total Assets Under Management (AUM), Number of portfolios	Include staked and locked assets at full value, Account for DeFi positions at current value
Dispersion Measure	Internal dispersion statistics, 3-year standard deviation	Expect high dispersion in crypto given volatility, Document volatility sources and drivers
Required Disclosures	Firm definition, Fee schedule details, Valuation methodology	Cryptocurrency-specific risks, Custody arrangement descriptions, Pricing source documentation

10.6.4 PERFORMANCE REPORTING

All performance reports should be clear, accurate, and transparent including:

- Net-of-fee returns for all relevant periods (monthly, quarterly, yearly, since inception)
- Performance attribution explaining return sources and key drivers
- Risk metrics providing context (volatility, Sharpe ratio, maximum drawdown, correlation to benchmarks)
- Clear narrative explaining key performance drivers during period, market conditions affecting results, positioning changes
- Benchmark comparison with explanation of tracking differences
- Disclosure of any significant events affecting comparability (fee changes, strategy shifts, valuation adjustments)

Performance presentation enables investor evaluation only when complete, consistent, and verifiable. Selective disclosure—favorable periods only, gross returns without fee context, inappropriate benchmarks—undermines the transparency essential to fiduciary relationships. GIPS compliance, while not required, provides a framework for consistent, complete performance presentation. Best practice is establishing documented performance calculation methodology covering: return calculation method, benchmark selection rationale, fee treatment, composite construction (if applicable), and reconciliation to administrator-calculated returns. Performance presentations should include sufficient context—time periods, benchmarks, fee impact—for investors to evaluate results meaningfully.

10.6.5 BENCHMARK SELECTION

The lack of standard benchmarks for cryptocurrencies makes it difficult to measure performance accurately. Unlike the S&P 500, which effectively tracks US stocks, there is no single index that represents the entire crypto market. When choosing a benchmark, it is important to consider both how relevant it is and how easily available it is. Additionally, it is essential to clearly communicate any limitations of the chosen benchmark.

- Bitcoin as a simple but narrow benchmark for basic market exposure
- Bitcoin and Ethereum blended benchmarks providing broader representation
- Crypto market-cap weighted indices despite inclusion of questionable tokens
- Custom benchmarks with full methodology disclosure

- Absolute return targets when no relevant benchmark exists

Benchmark disclosures should clearly explain why the benchmark was chosen, including supporting analysis. They should also mention any limitations or biases, describe how calculations are done step-by-step, specify how often rebalancing occurs and the rules used, and highlight any major differences from the strategy being compared. The goal is to make the information clear and easy to understand for digital asset managers in the investment industry.

> Changing benchmarks to improve relative performance can seem manipulative at first. To avoid this impression, choose a suitable benchmark and stick with it consistently. Clearly explain any limitations of the benchmark. If you need to change benchmarks because of significant strategic shifts, show both the old and new benchmarks for the entire historical period. Provide detailed reasons for the change, including why the previous benchmark no longer fits and why the new one offers better measurement. Investors will closely scrutinize benchmark changes and may suspect manipulation unless you provide clear, legitimate business reasons for the switch.

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional allocators evaluate valuation through independent oversight, pricing methodology rigor, and NAV accuracy controls. Inability to demonstrate Valuation Committee independence, produce pricing challenge documentation, or explain variance resolution reveals valuation governance inadequacy.

Valuation Governance and Independence

- Describe your Valuation Committee structure and member qualifications. Investment team-dominated committees lack independence.
- How do you ensure independence from portfolio management? Committee members with investment responsibilities create conflicts.
- Walk through a recent pricing challenge and resolution process. Inability to provide example suggests either no challenges (unlikely) or inadequate documentation.

- What triggers manual pricing overrides and who approves them? Unauthorized overrides or unclear approval authority indicates weak controls.
- How do you handle new asset types without established methodology?

Pricing Methodology and Validation

- Explain your pricing hierarchy and level assignments. Show examples of complex valuations with supporting documentation.
- How do you validate prices across multiple sources? Single-source pricing without validation creates error risk.
- What pricing sources do you use and why were they selected?
- How do you handle illiquid assets and locked positions?

NAV Process and Controls

- Walk through your daily NAV calculation process step-by-step. Who calculates NAV—internal team or independent administrator?
- How do you reconcile with your administrator? Show recent reconciliation reports with variance analysis.
- What controls ensure NAV accuracy and how do you handle errors when discovered?

Performance Measurement

- How do you calculate returns across different holding periods? Are you GIPS compliant?
- What benchmark do you use and why? Explain your performance attribution methodology.
- Show comprehensive performance reports with attribution detail and complete fee disclosure.

Documentary Evidence Requirements

- Complete valuation policies and procedures
- Valuation Committee charter and meeting minutes from past year
- Price challenge log with resolution documentation
- Daily NAV reconciliation reports showing variance analysis
- Monthly performance attribution reports

- External audit confirmation letters and management responses
- GIPS compliance verification report (if applicable)

COMMON PITFALLS & REMEDIATION

- *Investment team controls valuation without oversight*. Portfolio managers who selected positions also determine their valuations—creating inherent conflict between accurate pricing and favorable performance presentation. Independence exists on paper but investment team influence dominates. Remediation: Establish Valuation Committee with genuine authority, including CFO, CRO, and at least one independent member. Investment team provides input but not voting power. Committee must demonstrate willingness to override investment team preferences when warranted.
- *Illiquid asset valuations lack documented methodology*. Level 3 assets valued using undocumented models or "judgment" without stated assumptions, comparable transactions, or sensitivity analysis. Valuations can't be replicated or challenged because methodology isn't written down. Remediation: Develop comprehensive methodology documentation for each illiquid asset type: valuation approach, key inputs and sources, assumptions with rationale, and sensitivity to key variables. Update when market conditions change materially. Committee should review methodology, not just output.
- *NAV calculated internally without independent verification*. Fund calculates its own NAV without administrator involvement—removing the independent check that catches errors and deters manipulation. Remediation: Engage qualified fund administrator for NAV calculation and reconciliation. Administrator should price independently using agreed methodology, not simply accept manager-provided prices. Investigate material variances between manager and administrator views before finalizing NAV.
- *Performance presented selectively*. Marketing materials show favorable periods while omitting drawdowns or underperformance. Time periods selected to maximize apparent returns. Investors can't assess true track record from incomplete data. Remediation: Present complete performance history from inception through current period—no gaps, no cherry-picked windows. Include worst drawdown, recovery periods, and comparison to relevant benchmarks across all periods. Apply same presentation standards regardless of whether results are favorable.

- *Pricing sources selected opportunistically*. Different sources used for same asset across periods, or sources chosen based on which produces preferred price. Hierarchy exists in policy but isn't followed consistently. Remediation: Document binding pricing hierarchy by asset type specifying primary source, secondary source, and escalation procedures. Require Valuation Committee approval and documented rationale for any deviation from hierarchy. Monitor for patterns suggesting selective source application.
- *Performance reporting lacks transparency*. Reports show returns without explaining calculation methodology, fee treatment, benchmark selection rationale, or factors affecting comparability. Investors can't evaluate what numbers actually represent. Remediation: Disclose clearly: gross vs. net returns, calculation methodology (time-weighted vs. money-weighted), benchmark selection rationale, fee application, and any events affecting period comparability. Consistency across periods enables meaningful evaluation.
- *No process for identifying pricing anomalies*. Unusual prices accepted without challenge because no systematic review exists. Errors, stale prices, or manipulated inputs go undetected until material impact surfaces. Remediation: Implement automated exception reporting flagging prices outside tolerance bands, stale prices, and significant day-over-day movements. Maintain price challenge log documenting each exception, investigation performed, and resolution. Review exception patterns for systematic issues.
- *Valuation models never independently validated*. Models built by investment team used without independent review of methodology, inputs, or outputs. Model weaknesses or errors persist because no one outside the team examines them. Remediation: Conduct independent model validation annually—either by internal risk function or external party. Test key assumptions, verify input sources, and back-test against subsequent observable transactions where possible. Present validation findings to Valuation Committee with required remediation for identified issues.

KEY CONTROLS AND DOCUMENTATION

Document Type	Purpose	Update Frequency	Ownership
Valuation Policy	Comprehensive pricing methodology and governance framework	Annual review with interim updates	CFO/Valuation Committee
Pricing Manual	Detailed procedures for each asset type and scenario	Quarterly review with ad hoc updates	Finance Team
Source Documentation	Pricing source selection criteria and hierarchy	Semi-annual review	Operations
Committee Charter	Valuation committee governance and authority matrix	Annual review	Board of Directors
Price Challenge Log	Record of pricing disputes, investigations, resolutions	Ongoing contemporaneous documentation	Administrator/Finance
Override Documentation	Manual pricing interventions with full justification	Per occurrence with approval	Valuation Committee
NAV Reconciliation	Daily shadow NAV reconciliation and variance analysis	Daily with monthly trend analysis	Finance Team
Performance Reports	Monthly performance, attribution, and risk metrics	Monthly with quarterly comprehensive review	Finance Team
Validation Reports	Price validation exceptions and resolution tracking	Daily with weekly summary	Operations

Document Type	Purpose	Update Frequency	Ownership
Audit Findings	Valuation audit results and remediation plans	Annual with interim updates	External Auditor
Methodology Changes	Documentation of methodology updates and rationale	Per change with committee approval	Valuation Committee
Back testing Analysis	Historical accuracy assessment and model validation	Quarterly with annual comprehensive review	Risk Management
GIPS Compliance Manual	Policies and procedures for GIPS compliance	Annual review with updates as needed	Compliance Officer
Benchmark Documentation	Benchmark selection rationale and limitations	Annual review	Investment Team
Error Correction Log	Material errors, corrections, prevention measures	Ongoing documentation	Compliance Officer

STANDARD 11: TREASURY CONTROLS

Firms must implement strong treasury controls. This includes multi-layer authorization and verification for all fund transfers and cash movements; segregation of duties for cash management functions to prevent fraud; and fraud prevention and detection controls including transaction monitoring. Firms must maintain diversified banking relationships with regular monitoring of bank creditworthiness and document procedures for cash movements and reconciliation with appropriate approval workflows.

Treasury management in the digital asset sector bridges the gap between traditional banking and crypto-native infrastructure. Maintaining stable banking relationships remains a significant hurdle, as many financial institutions continue to avoid the sector due to perceived risk. While stablecoins offer a critical alternative for managing cash within the crypto ecosystem, they introduce their own set of counterparty risks that require constant oversight. The 2023 failures of Silvergate Bank and Signature Bank underscored the danger of banking concentration: firms reliant on a single institution risked losing all "on-ramp" and "off-ramp" capabilities overnight. Similarly, the 2022 collapse of TerraUSD demonstrated that stablecoins are not created equal; algorithmic versions lacking 1:1 reserves pose vastly higher risks than those backed by liquid, high-quality assets.

Standard 11 mandates robust treasury practices designed for resilience. This involves diversifying banking relationships across multiple jurisdictions to prevent a single point of failure and conducting rigorous due diligence on any provider facilitating the movement of fiat currency. It also requires a proactive assessment of stablecoin risk, focusing on the transparency of reserve backing and the reliability of redemption mechanisms. Firms must implement strict internal treasury controls, including the mandatory segregation of duties and dual authorization for every transaction, ensuring that no single individual can unilaterally move capital.

Effective treasury management operates on the assumption that disruptions in banking or stablecoin stability are inevitable. To meet this standard, firms must diversify their relationships before a crisis occurs, rather than reacting to one. Resilience is built through daily account reconciliation, continuous evaluation of stablecoin reserve attestations, and the maintenance of a "liquidity ladder" that ensures immediate access to operating capital. While diversification may increase operational complexity and overhead, it is a necessary safeguard against the catastrophic risk of being "de-banked" or holding impaired stablecoin assets.

11.1 BANKING RELATIONSHIPS

Stable and reliable banking relationships are the lifeline of a digital asset firm's "fiat" operations. However, traditional banks often remain hesitant to engage with the sector due to regulatory shifts and reputational concerns. This scarcity of services makes diversification difficult yet essential; relying on a single institution creates a critical point of failure where a sudden "de-banking" event can paralyze a firm's ability to pay expenses or fulfill investor redemptions. Investment managers must proactively build a network of multiple banking partners across varied jurisdictions to ensure operational continuity.

11.1.1 BANK SELECTION AND DUE DILIGENCE

A formal process for selecting and monitoring banking partners is required to mitigate counterparty risk. Following the Digital Asset Banking Act of 2026, institutions must be evaluated on their ability to maintain full reserves and their commitment to transparency.

Critical Assessment Areas:

- *Industry Expertise:* Verify the bank's track record with digital asset firms. They must demonstrate a capacity for high-volume, rapid settlements and an understanding of on-chain/off-chain reconciliation.
- *Financial & Capital Standing:* Review regulatory capital ratios and financial stability. Under current standards, firms should prioritize banks that maintain a Common Equity Tier 1 (CET1) ratio well above the regulatory minimum, typically targeting levels above 14% to ensure a buffer against market volatility.
- *Regulatory Status & Compliance:* Confirm the bank's charter (Federal vs. State) and FDIC insurance status. Assess the strength of their BSA/AML program specifically regarding digital asset "on-ramps," ensuring they utilize modern blockchain intelligence tools for transaction monitoring.
- *Relationship Stability:* Investigate the bank's history of "off-boarding" crypto clients. Managers should evaluate the bank's board-level commitment to the sector to avoid sudden service terminations.
- *Technology & API Integration:* Evaluate the bank's technological maturity. Institutional-grade partners should provide API access for automated reconciliations and support international payment rails (e.g., Swift, FedNow) with competitive cut-off times.

11.1.2 DIVERSIFICATION OF BANKING RELATIONSHIPS

Firms must diversify their banking footprint to avoid over-reliance on any single provider or regulatory jurisdiction.

Multi-Bank Requirements: Maintain active relationships with at least 2–3 institutions simultaneously. These accounts should be "warm," meaning they process regular transaction flows rather than sitting dormant, to ensure the relationship remains active and familiar to the bank's compliance team.

Target Balance Allocation:

- Primary Bank: 40–50% of cash holdings.
- Secondary Bank: 30–40% of cash holdings.
- Tertiary Bank: 10–20% (serving as a ready-to-use backup).

Operational Readiness Testing: Conduct monthly test transactions (Wire, ACH) across all banking partners to verify system uptime and compliance workflows.

Contingency & Exit Planning: Maintain documented "break-the-glass" procedures for rapid fund migration if a primary bank fails or issues an exit notice. This includes pre-vetted alternative providers and pre-authorized communication templates for investors and service providers.

> Banking concentration creates operational risk that may not be apparent until crisis. The 2023 failures of crypto-focused banks left firms with concentrated banking relationships unable to access funds or execute transactions—in some cases creating existential challenges. Cash diversification across banking partners provides resilience that single-bank relationships cannot. Best practice is maintaining relationships with multiple banking partners and distributing operating cash to avoid excessive concentration. For each banking relationship, understand contingency options if that relationship terminates. Firms that survived the 2023 banking disruptions generally had diversified relationships enabling rapid transition when problems emerged.

11.2 FIAT ON-RAMPS AND OFF-RAMPS

Fiat on-ramps and off-ramps serve as the critical "digital plumbing" connecting the traditional financial system to the cryptocurrency market. These gateways facilitate the conversion of government-issued currency into digital assets and vice versa. In today's market, these services are provided by a diverse array of entities—including centralized exchanges, OTC desks, stablecoin issuers, and specialized payment processors—each with distinct regulatory profiles, cost structures, and settlement risks. For institutional managers, selecting the right mix of providers is a strategic decision that directly impacts portfolio liquidity and operational cost.

11.2.1 ON-RAMP AND OFF-RAMP PROVIDERS

Institutional conversion requires bridging legacy banking rails (like SWIFT, FedNow, or SEPA) with high-throughput blockchain networks. Managers must evaluate providers based on transaction speed, liquidity depth, and total cost of ownership (TCO).

- *Centralized Exchanges (CEXs):* These are the most common entry points, offering familiar deposit/withdrawal interfaces. While they provide high convenience, they create custodial risk during the "holding" period and processing times can range from instant for wires to several days for ACH.
- *OTC (Over-the-Counter) Desks:* Best suited for high-volume conversions (typically $100k+). OTC desks provide relationship-based service with reduced price slippage and the ability to lock in rates before final settlement.
- *Stablecoin Issuers:* Direct "mint and redeem" relationships with regulated issuers (e.g., Circle) eliminate the exchange intermediary. This is often the preferred route for large treasury movements, as it leverages the GENIUS Act framework for 1:1 asset redemption.
- *Prime Brokers:* Integrated providers that offer fiat services alongside custody and execution. While fees may be higher, prime brokers reduce operational complexity by consolidating counterparty count into a single relationship.
- *Traditional Brokerages:* Established firms that have integrated digital asset access. These are useful for managers who prefer working within familiar regulatory structures, though they may offer a more limited selection of tokens.

11.2.2 DUE DILIGENCE AND MONITORING

Due to the heightened fraud risk and regulatory scrutiny associated with fiat-crypto movement, due diligence for ramp providers must be exhaustive. Failures in this area can lead to "liquidity bottlenecks," compliance violations, or even the loss of underlying banking rails.

Key Due Diligence Criteria:

- *Regulatory Status:* Verify that the provider holds necessary Money Transmitter Licenses (MTL) or is registered as a Virtual Asset Service Provider (VASP). Under current standards (like the CLARITY Act), providers must show clear evidence of federal and state-level compliance.
- *Compliance Infrastructure:* Evaluate the provider's AML/KYC program. This includes their ability to comply with the Travel Rule, which requires sharing originator and beneficiary information for transfers above certain thresholds.
- *Security & Fraud Controls:* Assess their transaction monitoring tools and internal "four-eyes" approval processes. Look for institutional-grade certifications such as SOC 2 Type II.
- *Operational Reliability:* Review documented uptime statistics and historical settlement performance. The provider must demonstrate the ability to process transactions predictably, even during periods of extreme market volatility.

Ongoing Monitoring: Monitoring does not end at onboarding. Managers must continuously track provider health, looking for "red flags" such as sudden changes in withdrawal timeframes, regulatory enforcement actions, or shifts in the provider's banking partners.

> Many investment managers focus only on the fees charged by on-ramp and off-ramp providers, but they often overlook hidden risks. A provider offering low fees might have weak compliance programs, which can lead to regulatory issues and disrupt operations. Similarly, a provider with limited operational capacity may struggle during periods of high transaction volume. To manage these risks, investors should request a comprehensive list of providers along with due diligence documents, details of transaction volumes to ensure diversification, and assessments of compliance and operational capabilities. They should also review procedures for handling provider disruptions. During due diligence, a key question to ask is: '*What happens if your main on-ramp provider becomes unavailable? How quickly can you switch to an alternative?*' If a provider cannot demonstrate backup options or shows long transition times, it indicates potential operational vulnerabilities.

11.3 STABLECOIN MANAGEMENT

Stablecoins are digital assets that aim to keep their value stable by being linked to traditional currencies like the US dollar. They are important for financial markets because they allow quick transactions, operate around the clock, and help manage cash in the crypto space. However, different stablecoins have different structures, which means they carry different levels of risk. For example, TerraUSD's failure showed that stablecoins without reserves, called algorithmic stablecoins, are very different from those backed by real assets. It is important for investment managers to carefully evaluate stablecoins to understand their risks and make informed decisions about their use in financial strategies.

TABLE 1: STABLECOIN TYPES

Type	Characteristics and Risk Profile
Fiat-Backed	Backed 1:1 by fiat currency reserves held in bank accounts or short-term securities. Examples: USDC, USDT. Lowest risk when reserves properly segregated and attested. Key risks: issuer insolvency, reserve custody bank failure, reserve composition changes, redemption mechanism restrictions. Monthly attestations verify reserve backing.
Crypto-Collateralized	Backed by cryptocurrency collateral typically over-collateralized to absorb volatility. Example: DAI. Moderate risk depending on collateral quality and liquidation mechanisms. Key risks: collateral value decline, liquidation cascade during volatility, smart contract vulnerabilities, oracle manipulation. Transparency through blockchain visibility.
Algorithmic	Maintain peg through algorithmic supply adjustments without reserve backing. Example: TerraUSD (failed). Highest risk with history of spectacular failures. Key risks: death spiral when confidence lost, no reserve backing for redemptions, complex mechanisms vulnerable to manipulation. Generally avoided by institutional investors post-Terra.

11.3.1 STABLECOIN DUE DILIGENCE

A thorough evaluation of a stablecoin must move beyond its "market peg" to analyze the underlying mechanics of its stability and the legal rights of the holder.

- *Reserve Assets:* Analyze the composition of the backing. Priority should be given to issuers holding 1:1 reserves in Cash and U.S. Treasury Bills. Evaluate the liquidity of these assets and verify if they are held in segregated, bankruptcy-remote accounts. Review the frequency and quality of independent attestations or audits (ideally monthly or real-time) to ensure reserves consistently match circulating supply.
- *Redemption Mechanism:* A stablecoin is only as good as the ability to exit. Determine who is eligible to redeem (e.g., all holders vs. only "Authorized Participants") and the typical timeframe for processing fiat payouts. Review historical performance during market stress to see if the issuer maintained a 1:1 redemption rate when liquidity was thin.
- *Regulatory Status:* Verify the issuer's licenses (e.g., NYDFS BitLicense or Trust Charter). Regulatory oversight ensures minimum capital requirements and consumer protections. Review the Terms of Service to clarify whether holders have a direct legal claim on the underlying reserves.
- *Issuer Financial Condition:* Assess the issuer's business model and capitalization. A stable issuer should have diversified revenue sources and reputable institutional shareholders, reducing the risk of a "run" caused by the issuer's own insolvency.
- *Technology and Security:* For blockchain-based assets, review smart contract audits from reputable firms. Evaluate the "mint and burn" controls to ensure no single party can unilaterally inflate the supply, and check the historical reliability of the protocol during high-volume periods.

11.3.2 STABLECOIN EXPOSURE LIMITS

To mitigate the risk of a stablecoin "de-pegging" event, firms must implement and enforce clear concentration limits.

Individual Stablecoin Limits: Maximum exposure to a single asset should be capped based on its risk tier:

- *Tier 1 (Fiat-Backed):* Well-established, regulated stablecoins (e.g., USDC) may have limits up to 30–40% of NAV.
- *Tier 2 (Emerging/Collateralized):* Newer or crypto-collateralized assets should be limited to 5–10%.
- *Prohibited Assets:* Algorithmic stablecoins without 1:1 liquid reserve backing should generally be avoided for institutional treasuries.

Aggregate Stablecoin Limits: Define a total cap for all stablecoin holdings combined to prevent an over-concentration in "synthetic" cash versus actual fiat banking balances. This forces a balance between operational speed and capital safety.

Dynamic Adjustment: Limits are not static. The operations team must review these caps monthly or immediately upon news of reserve discrepancies, regulatory actions, or redemption delays. Any decision to reduce a limit must be documented and executed across the entire portfolio.

> The collapse of TerraUSD in 2022 highlighted that not all stablecoins are the same. Algorithmic stablecoins, which do not have real-world reserves backing them, behave very differently from fiat-backed stablecoins. When confidence in an algorithmic stablecoin drops, it can trigger a 'death spiral,' where selling pressure causes the coin to lose its peg faster instead of restoring it. Investment managers should evaluate stablecoins carefully. They should request a clear policy on stablecoin use, detailed documentation for each stablecoin they hold, current exposure levels with limits, and procedures for ongoing risk monitoring. During due diligence, a key question to ask is: "*How do you assess each stablecoin's risk? What makes them different? How would you handle a situation where a stablecoin starts losing its peg?*" Providing generic answers that treat all stablecoins the same indicates a lack of understanding of their different risk profiles. Proper assessment and understanding are essential for managing digital assets effectively.

11.4 CASH CONTROLS AND TREASURY OPERATIONS

Strong internal controls are essential for mitigating cash management risks. These controls are designed to prevent fraud, eliminate operational errors, and block unauthorized transactions while maintaining the velocity required for digital asset markets. The effectiveness of these controls depends on genuine independence; nominal controls—where one person effectively manages multiple stages of a transaction—provide only a false sense of security.

11.4.1 SEGREGATION OF DUTIES

Clear segregation of duties in cash management prevents single individual from controlling entire transaction cycle. Key segregations include:

- *Initiation vs. Approval:* The individual initiating a wire transfer, ACH movement, or stablecoin "burn/mint" instruction must be distinct from the individual

approving it. The initiator must document the business purpose and verified destination, while the approver independently validates the legitimacy of the request.

- *Custody vs. Authorization:* Personnel with direct access to banking portals or cryptographic keys must not have the authority to unilaterally authorize transactions. In high-stakes environments, access rights—rather than just job titles—should define authority, with oversight teams defining the policy engines and thresholds that the execution teams must follow.
- *Reconciliation Independence:* To prevent the masking of unauthorized activity, the individual performing reconciliations must be independent of both the initiation and approval functions. Any discrepancies or "breaks" must be escalated directly to senior management or the risk committee.

11.4.2 DUAL AUTHORIZATION

All outbound cash movements require approval of at least two authorized individuals. Authorization requirements should include:

Authorization Thresholds: While a minimum of two signers is required for all movements, higher-value transactions should trigger additional layers of scrutiny. For example:

- *Standard Movements:* 2-of-3 authorized signers.
- *Material Thresholds* (e.g., >$1M): Requires 3-of-5 signers, including a C-level executive (CFO or CEO).

Genuine Independence: To prevent collusion, signers should not have direct reporting relationships (e.g., a junior staff member should not be the sole approver for their direct supervisor's transaction).

Address Whitelisting: Approvers must verify that the destination address or bank account is on a pre-approved "whitelist." Any transfer to a new address must undergo a separate, higher-intensity verification process before the transaction can be initiated.

Immutable Audit Trail: All steps—from request to final execution—must be logged in an immutable system (often a SOC 1/SOC 2 audited environment) capturing the identity, timestamp, and rationale for each approval.

11.4.3 RECONCILIATION

Daily reconciliation is the "early warning system" for treasury operations. Waiting for month-end reconciliation allows errors to propagate and makes identifying the root cause of on-chain anomalies nearly impossible.

Three-Way Reconciliation: Institutional best practice requires a "three-way tie-out" comparing:

- *Internal Ledgers:* The firm's proprietary records of expected balances.
- *On-Chain Data:* Real-time blockchain balances for stablecoins and tokenized deposits.
- *Bank/Custodian Statements:* Official third-party records.

Bank Reconciliation: Compare internal cash records with bank statements daily. All variances must be investigated and resolved immediately, with outstanding items tracked until clearance.

Stablecoin Verification: For blockchain-native assets, internal balances must be reconciled against live blockchain data every 24 hours. Any "unexpected" transactions on-chain—even if they result in an increase in funds—must be investigated as potential control failures or security breaches.

Administrator Tie-Out: Internal cash positions should be reconciled with the fund administrator's records daily to ensure the accuracy of the Net Asset Value (NAV) calculation.

> Payment controls require segregation between initiation and approval—no single individual should be able to complete a payment unilaterally. This fundamental control prevents both fraud and error, ensuring every material payment receives independent review before execution. Best practice is implementing payment workflows with separate initiation and approval steps, enforced through system controls where possible. Approval authority limits should be documented, with higher-value payments requiring additional authorization. Periodic review of payment activity against expected patterns can identify anomalies warranting investigation.

11.5 BANKING RELATIONSHIP MANAGEMENT

Managing banking relationships for digital asset firms requires a proactive, partnership-oriented approach. Banks are under continuous pressure from regulators to scrutinize crypto-linked entities, even those with impeccable compliance records. As an investment manager, your objective is to demonstrate that your firm is a high-transparency, low-risk client that strengthens—rather than compromises—the bank's own safety and soundness profile. This requires a shift from viewing the bank as a mere service provider to treating it as a key stakeholder in your risk management framework.

11.5.1 BANKING RELATIONSHIPS

The primary challenge in these relationships is an information imbalance. Banks often lack a granular understanding of the specific technological controls and multi-layered compliance systems used by institutional digital asset managers.

To address this, your framework should focus on educating banking partners about digital assets, offering clear transparency to build trust, and showing that your operations meet high institutional standards. It is also important to have backup plans in case your efforts to educate do not succeed, ensuring continuous support and reassurance for your banking relationships.

TABLE 2: BANKING RELATIONSHIP LIFECYCLE

Relationship Phase	Key Activities	Primary Objectives	Success Metrics
Initial Onboarding	Comprehensive due diligence package preparation, educational sessions about operations, facility site visits when practical, reference provision from existing banks	Establish institutional credibility, demonstrate robust controls, build personal relationships	Account approval achieved, full-service scope obtained, competitive fee agreement
Ongoing Management	Quarterly business review meetings, proactive compliance updates, transaction pattern education, rapid issue resolution	Maintain confidence levels, prevent relationship concerns, deepen relationship quality	Consistent service quality, fast response times, extended relationship tenure

Relationship Phase	Key Activities	Primary Objectives	Success Metrics
Risk Monitoring	Service degradation detection, policy change monitoring, enhanced review identification, relationship manager changes	Early warning detection, proactive response preparation, contingency plan activation	Advance termination notice, smooth transition management, zero operational impact
Termination Management	Professional notice acknowledgment, timeline extension negotiation, complete asset transfer, proper account closure	Professional relationship exit, complete fund transfer, clean documentation	Account closure confirmation, no asset losses, potential future relationship

Effective relationship management is a cornerstone of successful fiduciary practices, especially within the realm of digital asset management. It helps your firm distinguish itself as a trustworthy and reliable client in a highly competitive industry where trust and transparency are paramount. Consistent and clear communication demonstrates professionalism and fosters confidence among your partners and clients. Regular updates, such as quarterly reports, are essential for keeping relationship managers well-informed about your firm's activities, growth trajectory, and strategic initiatives. Educating your relationship managers and relevant stakeholders about transaction patterns is equally important. Understanding the typical transaction behaviors associated with digital assets—such as large international transfers, frequent transactions, and specific transfer patterns—helps banks and financial institutions comprehend your business needs. This knowledge reduces the likelihood of suspicion or unnecessary scrutiny, facilitating smoother operational processes.

11.5.2 BANKING CONTINGENCY PLANNING

Banking termination in the digital asset sector is rarely an isolated event; it often stems from broader regulatory shifts or internal bank policy changes. A systematic response prevents operational paralysis and preserves the firm’s ability to fulfill its fiduciary obligations. Early

detection is critical, as warning signs often precede formal termination notices by weeks, providing a window for proactive preparation.

Termination Warning Indicators

Firms must train treasury and compliance staff to recognize "soft" signals that a relationship is deteriorating:

- *Enhanced Due Diligence (EDD) Escalation:* Requests for information that go beyond standard annual reviews, particularly those focused on downstream customer activity or specific blockchain transaction types.
- *Transaction Friction:* A measurable increase in the frequency of "flagged" wires, manual documentation requests for routine ACH movements, or unexplained processing delays.
- *Service Degradation:* Slower response times from the institutional desk, limited access to new features (e.g., API keys), or the sudden removal of previously approved payment rails.
- *Personnel Shifts:* Changes in relationship management, particularly a move to less experienced staff or a "generalist" desk that lacks digital asset expertise.
- *Policy "Clarification":* New internal bank circulars or updated terms of service that restrict "high-risk" activities or specifically cite new interpretations of the Digital Asset Banking Act of 2026 as a reason for service limitations.

Termination Response Protocol

When a formal termination notice arrives—typically providing a 30-to-60-day window, though sometimes requiring immediate closure—the following protocol should be activated:

1. *Professional Acknowledgment:* Respond to the notice without emotional or legal confrontation. Maintaining a professional tone preserves the possibility of negotiating a timeline extension for orderly fund migration.

2. *Immediate Backup Activation:* Activate the "warm" secondary and tertiary accounts established. Direct all new incoming wires to these alternative venues immediately.

3. *Stakeholder Notification:* Inform the fund administrator, legal counsel, and the Board. Manage investor communication carefully, framing the transition as an execution of the firm's documented Contingency Plan rather than an emergency.

4. *Fund Liquidation & Transfer:* Prioritize the movement of large fiat balances and stablecoin reserve holdings. Ensure all funds are wired to the new banking partners

with confirmed receipt well before the deadline to prevent assets from being frozen in a "suspense account" during the closure process.

5. *Operational Updates:* Update all direct debit instructions, management fee accrual accounts, and payroll systems to ensure no service provider payments fail during the transition.

6. *Counterparty Alignment:* Notify key OTC desks and exchanges of the change in "settlement instructions" to ensure trading activity remains uninterrupted.

Transition Execution & Audit

To ensure a "clean break" and prevent future operational or regulatory issues:

- *Statement Preservation:* Download and secure the complete transaction history and all audited statements. These are essential for upcoming year-end audits and tax filings.
- *Closure Confirmation:* Obtain a formal "Account Closure Letter" from the bank to document that the relationship ended in good standing and that all client obligations were satisfied.
- *Process Review:* Following the transition, the Treasury Committee should conduct a "Post-Mortem" to identify the root cause of the termination and update the Bank Selection Criteria to avoid similar risks in the future.

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional allocators evaluate cash management through banking diversification, stablecoin risk assessment, and treasury control rigor. Inability to demonstrate multiple banking relationships, produce stablecoin due diligence, or explain dual authorization procedures reveals inadequate cash management controls.

Banking Relationships and Diversification

- Who are your banking partners and what is your process for selecting and monitoring them?
- How many active banking relationships do you currently maintain? Single banking relationships create existential vulnerability.
- Describe any past banking relationship terminations and your response. How you handled disruptions reveals crisis management capability.

- How do you manage banking concentration risk operationally? What specific contingency plans exist for banking disruptions?
- How do you manage exposure to fiat on-ramps and off-ramps? Provide list of providers and due diligence documentation.

Stablecoin Risk Management

- What is your policy on stablecoins and what is your current exposure to each? Firms treating all stablecoins as equivalent ignore material counterparty risk differences.
- Walk through your stablecoin due diligence—what analysis of reserve backing, redemption mechanisms, and issuer financial condition supports usage decisions?
- What ongoing monitoring occurs for stablecoin risks? Static assessments without continuous monitoring miss emerging threats.
- What exposure limits apply to each stablecoin based on risk assessment?

Treasury Controls and Authorization

- Walk through your cash management controls including segregation of duties and authorization requirements.
- What is your process for authorizing wire transfers and cash movements? Single-person authorization indicates inadequate fraud prevention.
- Who can initiate, approve, and execute cash movements? Lack of genuine segregation creates fraud vulnerability.
- Provide sample bank account reconciliations demonstrating daily reconciliation discipline.
- How quickly are reconciliation breaks investigated and resolved? Delayed investigation allows errors to compound.

Fraud Prevention and Detection

- What fraud awareness training do you conduct and how frequently? Untrained staff represent primary fraud vulnerability.
- Describe specific fraud attempts you have successfully prevented. Inability to cite examples suggests either perfect security (unlikely) or undetected attempts.
- How do you detect transaction anomalies systematically? Manual review without automated detection misses sophisticated fraud.
- What red flags trigger enhanced scrutiny and investigation?

- Show your documented incident response plan and testing results. Untested plans fail during actual fraud events.

Documentary Evidence Requirements

- Cash management policy with control procedures and authorization matrices
- List of all banking partners and on-ramp/off-ramp providers with due diligence files
- Stablecoin policy and current exposure report by stablecoin with risk ratings
- Stablecoin due diligence documentation including reserve analysis and ongoing monitoring
- Sample bank reconciliations demonstrating daily discipline with break resolution tracking
- Wire transfer authorization logs showing dual approval and segregation of duties
- Fraud prevention training records and incident response testing documentation
- Banking relationship contingency plans with testing results

---

COMMON PITFALLS AND REMEDIATION

- *Banking concentrated with single provider.* All operating cash and investor flows through one bank—creating existential risk if that relationship terminates or bank fails. The 2023 failures of Silvergate and Signature left firms with concentrated banking unable to operate. Remediation: Maintain relationships with at least two banking partners, with operating cash distributed to avoid single-bank dependency exceeding 50%. Test backup relationships periodically—a backup you've never wired to may not work when needed urgently.
- *Stablecoins treated as equivalent to cash.* All stablecoins used interchangeably without assessing reserve composition, attestation quality, redemption reliability, or regulatory status. Material differences in risk profile ignored for operational convenience. Remediation: Conduct due diligence on each stablecoin used: reserve composition and verification, attestation frequency and auditor quality, redemption track record, and regulatory standing. Set exposure limits reflecting risk assessment. Avoid algorithmic stablecoins or those lacking credible reserve verification.

- *Dual authorization is nominal*. Two signatures required but both approvers report to the same person, or one routinely defers to the other, or CEO can override when convenient. The control exists in procedure but not in practice. Remediation: Ensure genuine independence: approvers with separate reporting lines and no ability for one to pressure the other. Eliminate override authority entirely—no exceptions for urgency or seniority. Test periodically that system controls actually enforce dual authorization.

- *Reconciliation delayed or incomplete*. Cash and stablecoin balances reconciled weekly or monthly rather than daily. Breaks accumulate undetected, errors persist, and fraud risk increases with each day of delay. Remediation: Reconcile all cash and stablecoin positions daily against independent sources. Investigate variances immediately—not flagged for later review. Assign reconciliation to operations or finance function independent from those initiating transactions.

- *No contingency for banking or stablecoin disruption*. Assumption that current banking and stablecoin arrangements will remain available. When disruption occurs, scrambling for alternatives under time pressure while operations are impaired. Remediation: Document contingency procedures for banking disruption (primary bank fails or terminates relationship) and stablecoin stress (depeg, redemption halt, regulatory action). Identify specific alternatives and required transition steps. Test annually that contingency paths remain viable.

- *Fiat on/off-ramp providers inadequately diligenced*. Conversion providers selected for speed and cost without assessing licensing, compliance programs, security controls, or operational reliability. Provider failure or regulatory action disrupts fund operations. Remediation: Conduct due diligence on all on/off-ramp providers covering: regulatory licenses and compliance status, AML program adequacy, security practices, and operational track record. Diversify across providers to avoid single-source dependency for fiat conversion.

- *Segregation of duties documented but not enforced*. Policy requires separation between transaction initiation and approval, but system access or informal practices allow individuals to perform both functions. Control exists on paper only. Remediation: Verify segregation through control testing—attempt transactions that should be blocked and confirm they are. Enforce role-based system permissions that technically prevent circumvention. Audit access logs for patterns suggesting control bypass.

- *Cash control procedures undocumented or unclear*. Treasury operations rely on institutional knowledge rather than written procedures. Approval authorities undefined, escalation paths unclear, responsibilities assumed rather than assigned. Remediation: Document treasury procedures covering: approval authorities by transaction type and amount, segregation requirements,

reconciliation responsibilities, and escalation procedures. Review annually and update when personnel or systems change. Ensure documentation enables continuity if key personnel are unavailable.

- *Treasury operations lack independent oversight.* Treasury function operates without periodic review by compliance, risk, or internal audit. Control weaknesses persist undetected because no one outside treasury examines the operation. Remediation: Implement periodic treasury review—quarterly by risk or finance function, annually by internal audit or external party. Assess control design and operating effectiveness. Track findings to remediation with defined timelines and accountability.

KEY CONTROLS & DOCUMENTATION

Document Type	Purpose	Update Frequency	Ownership
Cash Management Policy	Comprehensive framework for all cash operations and controls	Annual review	CFO
Wire Transfer Procedures	Detailed wire controls, approval processes, and verification requirements	Quarterly review	CFO/Chief Operating Officer (COO)
Banking Relationship Matrix	Complete list of banking relationships, contacts, and service scope	Monthly updates	Treasury Function
Authorized Signatory List	Current approval authorities with dollar limits	Real-time updates	CFO
Fraud Prevention Procedures	Anti-fraud controls, detection systems, and training requirements	Semi-annual review	Security Officer
Cash Forecast Model	Daily, weekly, and monthly liquidity projections	Daily updates	Treasury Function

Document Type	Purpose	Update Frequency	Ownership
Wire Transfer Log	Complete record of all wire transfer activity	Real-time capture	Operations Team
Banking Contingency Plan	Response procedures for banking relationship termination	Quarterly review	CFO
Foreign Exchange Policy	FX procedures, controls, and exposure management	Annual review	CFO
Reconciliation Reports	Daily cash reconciliation across all bank accounts	Daily production	Operations Team
Fraud Incident Log	Record of attempted and successful fraud incidents	Ongoing documentation	Security Officer
Training Records	Fraud awareness and security training completion documentation	Annual updates	Human Resources/Security
Vendor Payment Records	Approved vendors with verified payment instructions	Ongoing maintenance	Finance Team
Banking Fee Analysis	Cost analysis across all banking relationships	Quarterly assessment	Treasury Function
Emergency Contact List	24/7 contact information for crisis response	Quarterly verification	COO

STANDARD 12: TECHNOLOGY & CYBERSECURITY

Firms must maintain resilient technology infrastructure. This includes appropriate redundancy and failover capabilities; comprehensive cybersecurity program with regular testing, updates, and threat monitoring; and business continuity and disaster recovery plans for all critical functions with regular testing. Firms must establish incident response procedures with defined roles, escalation paths, and communication protocols and maintain a vendor management framework for all technology service providers with ongoing performance monitoring.

Technology infrastructure in digital asset management operates under constant threat from sophisticated cyberattacks targeting high-value, liquid assets. Because digital assets are bearer instruments, a single security breach can result in the instantaneous and permanent theft of capital. Unlike traditional finance, where centralized ledgers allow for the reversal of unauthorized transactions, blockchain-based assets are notoriously difficult to recover once moved. Firms must operate nonstop, processing transactions within milliseconds to remain competitive in a 24/7 global market that lacks traditional maintenance windows.

Standard 12 mandates that firms build resilient, institutional-grade technology systems supported by rigorous security protocols and documented continuity plans. This framework requires the implementation of layered cybersecurity defenses—a "defense-in-depth" strategy—across all hardware, software, and human workflows. Critical requirements include automated failover processes, regular third-party penetration testing, and a comprehensive disaster recovery plan that is tested under simulated stress. Independent validation, such as SOC 2 Type II examinations, is essential to prove that security controls are not just designed well, but are operating effectively over time. In this environment, resilience is defined by a firm's ability to detect and contain an inevitable breach within minutes.

Adhering to these standards requires a fundamental shift in perspective: technology must be viewed as a strategic core asset, not an operational overhead cost. Institutional-grade resilience demands continuous monitoring, immutable logging of all security events, and a commitment to ongoing investment in the security stack. Firms that treat cybersecurity as a cost-saving area risk catastrophic operational failure and will likely be disqualified from institutional mandates. Ultimately, a resilient technology system is the only reliable safeguard for protecting digital assets and maintaining the long-term trust of global allocators.

12.1 TECHNOLOGY INFRASTRUCTURE AND GOVERNANCE

Technology infrastructure constitutes the collection of hardware, software, and networks supporting investment operations. In the digital asset space, infrastructure must be designed for resilience, security, and scalability—capable of handling extreme market volatility, peak transaction loads, and component failures without service disruption. The quality of this infrastructure directly determines the firm's operational reliability, its security posture against sophisticated attackers, and its competitive execution capability.

12.1.1 TECHNOLOGY STACK

Institutional investment managers utilize a "best-of-breed" technology stack, blending proprietary tools with specialized third-party solutions. This modular approach allows for flexibility and integration while reducing the complexity that leads to operational instability.

- *Portfolio Management System (PMS):* Serves as the official system of record for all positions and transactions. It maintains a complete historical audit trail and integrates with accounting and reporting functions to provide real-time updates for rapid decision-making.
- *Order Management System (OMS):* Manages the entire order lifecycle. It is responsible for routing orders to various liquidity venues (exchanges, OTC desks) and supporting algorithmic execution. Crucially, the OMS performs pre-trade risk checks to prevent "fat-finger" errors or limit breaches.
- *Risk Management System:* Provides real-time risk calculations across the entire portfolio. It enables continuous limit monitoring with automated alerts, stress testing, and exposure aggregation across multiple venues and instruments.
- *Data Warehouse:* A centralized repository for market data, transaction history, and risk metrics. This layer supports advanced analytics and regulatory reporting while implementing data quality controls to ensure "single version of truth" accuracy.
- *Core Infrastructure Components:* High-availability servers with automated redundancy, network failover capabilities, and database replication. This also includes the integration of secure cloud services and immutable offsite backups for disaster recovery.

12.1.2 TECHNOLOGY GOVERNANCE

A formal technology governance framework, approved by the Board, ensures that technology decisions are aligned with business objectives and regulatory requirements. Governance provides the accountability and transparency necessary to manage a high-stakes digital infrastructure.

- *Technology Strategy:* A long-term roadmap that dictates "build versus buy" decisions and infrastructure architecture (e.g., hybrid cloud vs. on-premise). It sets investment priorities and budget allocations to ensure the firm stays ahead of the technological curve.
- *Policies and Procedures:* Documented standards for data governance (classification and access), change management (testing and approval), and incident response. This includes rigorous Vendor Management—performing deep-dive due diligence on any third-party technology provider.
- *Technology Committee:* A formal body responsible for oversight. The committee approves major investments, reviews security posture, and evaluates incident reports.
    - Cadence: Meetings should occur at least quarterly.
    - Documentation: All decisions and strategy shifts must be formally minuted for audit purposes.

> Technology decisions made without business risk context, or business decisions made without technology input, create blind spots. Technology risk—including cybersecurity, system reliability, and key management—requires visibility at the highest governance levels and clear accountability for risk management. Best practice is ensuring technology risk is represented in board or senior management discussions, with clear accountability for cybersecurity and operational technology resilience. Material technology decisions—including security architecture, key management systems, and critical vendor selection—should receive appropriate governance review.

12.1.3 SYSTEM AVAILABILITY AND RECOVERY FRAMEWORK

Recovery goals in digital asset management must account for a market that never sleeps. Unlike traditional finance, there are no "market closes" or fixed maintenance windows.

Infrastructure must be designed for continuous operation, with recovery targets calibrated to prevent catastrophic losses in a 24/7 environment.

- *Recovery Time Objective (RTO):* Critical systems must have an RTO of less than one hour. This ensures that even during a major failure, the firm can regain market access and manage risk before price volatility causes significant NAV erosion.
- *Recovery Point Objective (RPO):* To maintain the integrity of high-frequency transaction data, the RPO is set at less than 15 minutes. This limits the potential for data "gaps" that could lead to inaccurate positioning or accounting errors.
- *Maximum Tolerable Downtime (MTD):* A limit of four hours is established to prevent irreversible reputational damage and systemic business failure.
- *Work Recovery Time:* Once systems are back online, operational staff should reach full productivity within two hours by reconciling any transactions that occurred during the outage.

TABLE 1. SYSTEM AVAILABILITY & RECOVERY HIERARCHY

System Category	Availability Target	Maximum Downtime	Recovery Approach
Trading Systems	99.95%	~4 minutes/month	Active failover, geographic redundancy, automatic rerouting
Critical Systems	99.99%	~26 seconds/month	Hot standby, real-time replication, instant failover
Data Systems	99.9%	~43 minutes/month	Multi-region backup, point-in-time recovery, read replicas
Support Systems	99.5%	~3.6 hours/month	Standard redundancy, manual failover, business-hours support

12.1.4 TECHNOLOGY STACK INTEGRATION

Institutional digital asset management requires “connected" architecture. The technology stack should not function as a series of isolated silos; rather, it must integrate seamlessly with existing asset management workflows to ensure data consistency and operational control.

Core Technology Components:

- *Execution Infrastructure:* Seamless connectivity to a diverse liquidity pool, including centralized exchanges (CEXs), decentralized exchanges (DEXs), OTC desks, and prime brokers.
- *Custody Integration:* Direct bridges between trading systems and qualified custodians or MPC-based wallet infrastructure to facilitate secure asset movement.
- *Data Aggregation:* Unified ingestion of market data, blockchain node snapshots, and real-time on-chain analytics to provide a single "source of truth."
- *Risk & Compliance:* Real-time engines calculating Value at Risk (VaR) and monitoring limits, integrated with wallet-screening tools to ensure all transactions meet AML standards.
- *Administration & Reporting:* Automated data flows to fund administration systems for NAV calculation, performance attribution, and investor reporting.

12.2 CYBERSECURITY PROGRAM

A robust cybersecurity program is the primary defense for protecting digital assets, sensitive data, and core operational systems. The program should align with recognized global standards—such as the NIST Cybersecurity Framework, ISO 27001, or CIS Controls—to ensure a structured and comprehensive approach. To remain effective in the evolving digital asset landscape, the program must be implemented consistently, tested under stress, and refined through continuous feedback loops.

12.2.1 KEY COMPONENTS OF A CYBERSECURITY PROGRAM

An institutional-grade cybersecurity program for digital asset managers integrates technology, process, and people to create a "defense-in-depth" architecture.

- *Asset Management:* Maintain a complete, live inventory of all hardware, software, and data. Assets are classified by criticality and sensitivity, with clear ownership assigned to ensure proper lifecycle management and decommissioning.
- *Access Control:* Implement the Principle of Least Privilege (PoLP)—granting users only the minimum access necessary for their roles. Mandatory Multi-Factor Authentication (MFA) is required for all systems, supported by regular role-based access reviews and enhanced monitoring for privileged accounts.

- *Data Encryption:* Protect data in transit using TLS 1.2 or higher and ensure data at rest is encrypted using industry-standard algorithms (e.g., AES-256). Robust key management, including scheduled rotation, is essential for maintaining encryption integrity.
- *Network Security:* Utilize network segmentation to isolate critical trading and custody systems from general office networks. This is bolstered by firewalls, intrusion detection systems (IDS), and specialized Denial of Service (DoS) protections to maintain availability during attacks.
- *Endpoint Security:* Deploy Endpoint Detection and Response (EDR) tools across all devices. This includes automated patch management, device encryption, and Mobile Device Management (MDM) with remote-wipe capabilities for lost or stolen hardware.
- *Security Monitoring:* Use a Security Information and Event Management (SIEM) system to aggregate and analyze logs in real time. This allows for automated alerting on suspicious activity and provides the forensic data necessary for post-incident analysis.
- *Employee Training:* Security awareness is a firm-wide responsibility. All staff must undergo regular training, including simulated phishing exercises. Developers should receive specialized training in secure coding practices to prevent vulnerabilities at the application layer.

12.2.2 THIRD-PARTY SECURITY TESTING

Independent validation is required to identify vulnerabilities before they can be exploited by malicious actors.

- *Penetration Testing:* Conduct annual "Red Team" simulations that attack the firm from both external and internal perspectives. Critical findings must trigger immediate remediation and a follow-up re-test.
- *Vulnerability Scanning:* Run automated, credentialed scans on a continuous or scheduled basis to identify unpatched software or misconfigurations. Remediation is prioritized based on the Common Vulnerability Scoring System (CVSS).
- *Social Engineering Testing:* Perform simulated phishing and "vishing" (voice-based) attacks to measure and improve employee vigilance. Results should inform future training sessions in a constructive, non-punitive manner.
- *SOC 2 Type II Audit:* Undergo an annual independent audit to verify the effectiveness of security, availability, and confidentiality controls over a 6-to-12

month period. This is an essential requirement for institutional allocators and serves as proof of a mature control environment.

> Cybersecurity programs focused solely on perimeter defense may provide insufficient protection against sophisticated threats. The assumption should be that determined attackers will eventually gain some access—effective security requires detection, containment, and response capabilities in addition to prevention. Best practice is implementing a security framework that addresses: prevention (access controls, network security, endpoint protection), detection (monitoring, anomaly detection, threat intelligence), and response (incident response procedures, recovery capabilities, communication protocols). Regular testing—including penetration testing and incident response exercises—validates that capabilities work as intended.

12.3 DIGITAL ASSET SECURITY OPERATIONS

Digital asset management introduces risks that extend beyond traditional cybersecurity into the realm of blockchain-specific vulnerabilities. These include smart contract exploits that can drain funds in seconds, Maximum Extractable Value (MEV) bots that manipulate transaction ordering for profit, and bridge failures that can permanently lock assets across chains. Because blockchain transactions are immutable and instantaneous, the window to react to an incident is virtually non-existent, making proactive operational security the only viable defense.

12.3.1 SMART CONTRACT SECURITY

Managing interactions with decentralized protocols requires a rigorous lifecycle approach to ensure that "code-based" counterparties do not compromise the portfolio.

- *Pre-Interaction:* Before deploying capital, firms must review independent audits, verify source code on blockchain explorers, and run simulations in "sandbox" environments. Risk is further mitigated by whitelisting specific contracts and implementing time-locks or multi-signature requirements for initial deposits.
- *During Interaction:* Use real-time transaction simulations to predict outcomes and prevent "reentrancy" or "flash loan" attacks. Standard controls include setting strict gas price ceilings and slippage limits to prevent MEV exploitation.

- *Post-Interaction:* Continuous monitoring of protocol health and governance proposals. Any anomaly should trigger automated "circuit breakers" to withdraw liquidity or revoke contract permissions immediately.

12.3.2 PRIVATE KEY AND WALLET SECURITY

Private key management is the most critical security function in digital asset operations. A compromise at this level results in binary failure: the total and irreversible loss of assets.

Key Generation and Storage:

- *Entropy and Randomness:* Keys must be generated using Hardware Security Modules (HSMs) that provide certified true randomness. Generation should occur in an "air-gapped" environment (disconnected from all networks) within a physically secure facility.
- *Ceremony Protocols:* Multiple authorized witnesses must be present during key generation to document the process and ensure no single individual can copy the key material.
- *Geographic Distribution:* Encrypted key shards or backups should be distributed across multiple secure, geographically diverse locations to prevent loss from a single localized disaster.

Key Usage Controls:

- *Multi-Signature (Multi-sig):* Mandate that a majority (e.g., 3-of-5) of authorized signers approve a transaction before it is broadcast to the network.
- *Whitelisting and Time-Locks:* Limit outbound transfers to pre-verified destination addresses. For material amounts, implement time-locks that delay execution for 24–48 hours, providing a window to cancel unauthorized movements.
- *Threshold Monitoring:* Automated systems should flag and halt transactions that deviate from historical patterns or exceed pre-set risk thresholds.

Access controls degrade over time without active management. Employees accumulate permissions for past projects and retain them indefinitely; departed employees may remain in systems longer than intended; privileged access may not be monitored appropriately. Regular access review prevents the accumulation of unnecessary access that increases attack surface. Best practice is implementing periodic access reviews (quarterly for privileged access, at least annually for general access), prompt termination procedures for departing employees (within 24 hours), and monitoring of privileged account usage. Access should be granted based on need, time-limited where appropriate, and removed when no longer required.

12.4 BUSINESS CONTINUITY AND DISASTER RECOVERY (BCP/DR)

The Business Continuity Plan (BCP) is a formal framework ensuring that the firm remains operational during major disruptions, such as cyberattacks, infrastructure failures, or regional disasters. In a 24/7 market, the plan must facilitate seamless operations without the luxury of "market holidays." Disaster Recovery (DR) focuses specifically on the technical restoration of systems to ensure data integrity and minimal downtime.

12.4.1 BCP/DR PLAN COMPONENTS

A comprehensive BCP/DR plan must define clear metrics and procedures to guide the firm through a crisis:

- *Recovery Time Objective (RTO):* The maximum allowable downtime for a system. For trading and key management, the RTO is typically under one hour; for non-critical reporting, it may be several hours.
- *Recovery Point Objective (RPO):* The maximum amount of data loss acceptable (measured in time). Critical transaction ledgers require an RPO of minutes to ensure no trades are "lost" during a failover.
- *Crisis Management Team:* A designated group with clearly defined roles and decision-making authority. This includes pre-defined communication templates for notifying investors, regulators, and service providers.
- *Step-by-Step Procedures:* Documented failover scripts that allow trained personnel to restore operations at a backup site or via cloud redundancy without improvisation.

12.4.2 BCP/DR TESTING

A BCP is only as effective as its last successful test. Firms must conduct regular exercises to validate their recovery capabilities:

- *Tabletop Exercises (Semi-Annual):* Discussion-based scenarios where the Crisis Management Team walks through their response to simulated events like a total exchange outage or a ransomware attack.
- *Functional Testing (Quarterly):* Isolating and testing specific components, such as verifying that off-site backups can be successfully restored and that redundant communication channels are functional.
- *Full Failover Exercises (Annual):* A complete "live" switch to disaster recovery systems to verify that the firm can meet its stated RTO and RPO under realistic conditions.
- *Post-Test Documentation*: Every test must produce a formal report identifying gaps or failures. Remediation plans with specific timelines must be reviewed and approved by the Board.

Many businesses focus their Business Continuity and Disaster Recovery (BCP/DR) plans only on major events like natural disasters. However, most disruptions are smaller and more common, such as hardware failures, software bugs, human mistakes, or vendor outages. A good BCP/DR plan should cover all types of disruptions, from minor issues to large-scale disasters. To evaluate a company's preparedness, assess whether they have a complete BCP/DR plan with clear recovery time objectives (RTO) and recovery point objectives (RPO), a testing schedule with recent test results, records of post-test fixes, and a history of incidents showing how well they recovered compared to their targets. Companies that cannot show evidence of testing or are defensive about issues found during testing may not be fully prepared. Having a plan without regular testing can give a false sense of security, so ongoing testing and updates are essential for effective business continuity management.

12.5 TECHNOLOGY GOVERNANCE AND VENDOR MANAGEMENT

Technology governance in digital assets must balance rapid innovation with rigorous operational control. The market evolves constantly, with new protocols and tools emerging weekly; however, each adoption increases operational complexity and the firm's attack surface. Robust governance enables firms to capture the value of innovation while maintaining the stability and security required to prevent destabilizing changes.

Vendor risk is especially acute in this sector. Many technology providers are early-stage companies that may pivot, fail, or be acquired. Over-reliance on a single vendor without documented alternatives creates significant concentration risk. Managers must extract maximal value from these partnerships while maintaining proactive contingency plans.

12.5.1 TECHNOLOGY GOVERNANCE FRAMEWORK

Change management is the organized process of adopting and updating technology to prevent disruptive failures while allowing for necessary improvements. This framework ensures that updates are controlled, tested, and reversible.

- *Standard Changes (Low Risk):* Routine, repetitive updates (e.g., standard security patches or UI adjustments) that follow an established procedure. These can be pre-approved and logged automatically.
- *Normal Changes (Medium Risk):* Business-related or architectural updates that require a formal Request for Change (RFC). These demand committee review, full sandbox testing, and a documented rollback plan.
- *Emergency Changes (Critical):* Urgent fixes required to address a security breach or system failure. These require expedited approval from senior leadership and a retrospective review within 24 hours of implementation.
- *Major Changes (High Risk):* Significant shifts, such as migrating to a new Order Management System (OMS) or changing custody providers. These require Board-level notification, phased rollouts (canary deployments), and comprehensive updated documentation.

12.5.2 VENDOR MANAGEMENT PROGRAM

Vendor oversight is risk-based, with the intensity of monitoring directly proportional to the vendor's criticality to firm operations. Following the Digital Asset Banking Act of 2026, managers must also ensure that third-party vendors—especially sub-custodians—meet the same "one-to-one" reserve and audit standards as the primary firm.

TABLE 2: TECHNOLOGY VENDOR MANAGEMENT MATRIX

Vendor Tier	Risk Level	Review Frequency	Oversight Requirements	Contingency Planning
Critical Vendors	Maximum risk	Quarterly comprehensive reviews	Continuous performance monitoring, Detailed service level agreement (SLA) tracking, Regular security assessments, Financial viability monitoring	Documented migration plans, Tested backup vendors, Data portability verified, Transition tested annually
Important Vendors	High risk	Semi-annual assessments	Performance tracking, Contract compliance monitoring, Annual security review	Transition strategy defined, Alternative vendors identified, Data export capability validated
Standard Vendors	Medium risk	Annual reviews	Basic performance tracking, Standard contract terms	Easy replacement options, Standard transition procedures
Commodity Vendors	Low risk	Minimal oversight	Basic performance tracking, Standard contracts	Multiple alternatives available, Simple replacement process

Vendor Assessment Dimensions

Before onboarding any technology provider, managers must evaluate the following dimensions to determine the appropriate risk tier:

- *Security Posture:* Reviewing SOC 2 Type II or ISO 27001 certifications and historical security incident response.
- *Financial Stability:* Evaluating funding rounds, revenue trends, and overall viability to ensure the vendor won't disappear during a market downturn.
- *SLA Performance:* Measuring uptime, API latency, and customer support responsiveness against institutional requirements.

- *Compliance & Legal:* Assessing adherence to data protection laws and the CLARITY Act requirements for digital asset intermediaries.
- *Exit Portability:* Verifying how easily data can be exported and migrated to a competitor if the relationship is terminated.

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional allocators evaluate technology through cybersecurity rigor and business continuity preparedness. Inability to produce penetration test results, demonstrate tested disaster recovery procedures, or explain technology governance reveals infrastructure inadequacy for managing digital assets.

Technology Infrastructure and Architecture

- Describe your technology architecture including network zones and security layers. Provide architecture diagram showing systems and security controls.
- How do you ensure high availability and prevent single points of failure? What redundancy exists across critical systems?
- How do you handle 24/7 operations given continuous market activity?
- What are your RTO and RPO targets for different system categories?

Cybersecurity Program

- What cybersecurity program do you maintain and what framework is it based on (NIST, ISO 27001, CIS Controls)?
- Walk through your security defense layers from perimeter to data protection.
- What penetration testing is performed, who conducts it, and what were recent findings? Provide most recent penetration test results.
- What is your SOC 2 status? Absence of SOC 2 for firms above $100M AUM signals inadequate security controls.
- How do you protect private keys and what controls govern usage?
- Describe a recent security incident and your response. Inability to provide example suggests inadequate incident tracking.

Digital Asset-Specific Security

- How do you evaluate smart contracts before interaction? What controls govern DeFi protocol interactions?

- Describe your wallet security architecture and transaction authorization procedures.
- What monitoring detects suspicious blockchain activity?

Business Continuity and Testing

- Provide your Business Continuity Plan. When did you last test it and what were the results?
- What disaster scenarios have you planned for including crypto-specific events?
- How would you respond to ransomware or extended outage?
- Walk through failover scenarios and demonstrate execution capability. Untested plans fail when needed.

Documentary Evidence Requirements

- Network architecture diagrams showing security zones and controls
- Technology governance framework and cybersecurity policy
- Recent penetration test results with findings and remediation
- SOC 2 Type II report (if applicable)
- Business Continuity Plan with defined RTOs and RPOs
- BCP test results and after-action reports with actual versus target metrics
- Incident response procedures and recent incident logs
- Vendor assessment documentation with risk ratings

COMMON PITFALLS AND REMEDIATION

- *Technology treated as cost center rather than infrastructure.* Underinvestment in systems, security, and personnel creates operational fragility that becomes apparent during growth, stress, or incident. Manual processes and outdated systems can't scale with AUM or withstand sophisticated threats. Remediation: Budget technology as operational infrastructure, not discretionary expense. Maintain documented technology roadmap covering planned upgrades, security investments, and capacity scaling. Benchmark spending against peers—significant underinvestment relative to AUM and complexity is a warning sign.

- *No independent control validation*. Firm asserts adequate controls but lacks independent verification. Without SOC 2 or equivalent examination, control effectiveness is self-assessed—providing limited assurance to allocators or regulators. Remediation: Engage qualified auditor for annual SOC 2 Type II examination once AUM exceeds $100M or institutional investors require it. Address findings with documented remediation and timelines. SOC 2 is increasingly table stakes for institutional allocators—absence raises questions.
- *Security testing infrequent or findings ignored*. Penetration testing performed once or sporadically, or critical findings deprioritized because remediation is inconvenient. Vulnerabilities persist until exploited. Remediation: Conduct penetration testing at least annually and after significant infrastructure changes. Remediate critical and high findings within defined timeframes (e.g., critical within 30 days). Track findings to closure with accountability—testing without remediation is security theater.
- *Business continuity plans untested*. BCP and disaster recovery procedures documented but never exercised. Assumptions about recovery time, system failover, and personnel availability unvalidated until actual disruption—when discovering gaps is too late. Remediation: Conduct full failover tests annually, verifying systems actually recover within defined RTO/RPO targets. Hold tabletop exercises semi-annually for scenarios requiring human decision-making. Document test results and remediate gaps before the real event.
- *Security awareness treated as compliance checkbox*. Annual training completed for the record but employees don't internalize threats or change behavior. Phishing simulations not conducted, or results not used to improve awareness. Remediation: Implement ongoing security awareness program: annual comprehensive training, regular phishing simulations with constructive follow-up, and reinforcement of key behaviors. Track metrics over time—click rates should decline. Foster culture where reporting suspicious activity is encouraged, not penalized.
- *Critical systems lack redundancy*. Key infrastructure—trading systems, custody access, communication platforms—has no backup. Single point of failure means single incident causes operational halt. Remediation: Identify all critical systems and implement redundancy: backup infrastructure, failover capability, alternative access methods. Document RTO for each critical system. Test failover periodically—redundancy that hasn't been tested may not work when activated.
- *No continuous security monitoring*. Security posture assessed periodically but no real-time visibility into threats, anomalies, or incidents. Breaches detected only when damage becomes obvious. Remediation: Implement continuous monitoring through SIEM or managed security service. Define alerting thresholds

and escalation procedures. Ensure 24/7 coverage appropriate to threat profile—attackers don't respect business hours. Test that alerts reach responders and trigger appropriate action.

- *Technology governance informal or absent*. No clear ownership of systems, vendors, changes, or security. Decisions made ad hoc, changes implemented without review, and accountability unclear when issues arise. Remediation: Assign clear technology leadership (CTO or designated technology lead) with defined responsibilities. Implement change management process requiring review and approval before production changes. Conduct quarterly technology reviews covering system health, security status, and upcoming requirements.
- *Infrastructure aging beyond secure lifecycle*. Legacy systems remain in production past vendor support dates or with unpatched vulnerabilities because replacement is disruptive or expensive. Technical debt accumulates until failure or breach forces action. Remediation: Maintain inventory of all systems with support status and patching currency. Establish refresh schedule aligned with vendor support lifecycles. Plan upgrades proactively—emergency replacement during incident is more disruptive and expensive than planned migration.

KEY CONTROLS AND DOCUMENTATION

Document Type	Purpose	Update Frequency	Ownership
Technology Policy	Comprehensive governance framework	Annual review	CTO
Security Policy	Security controls and procedures	Semi-annual review	CTO
Network Architecture Diagram	Current system architecture	Monthly updates	IT Operations
Asset Inventory	Complete technology asset register	Real-time maintenance	IT Operations
Incident Response Plan	Security incident playbooks	Quarterly review	IT Operations

Document Type	Purpose	Update Frequency	Ownership
Disaster Recovery Plan	System recovery priorities and procedures	Semi-annual review	CTO/COO
Business Continuity Plan	Operational continuity procedures	Annual review	COO
Vendor Registry	Vendor list with risk ratings	Monthly updates	Procurement
Change Management Log	Record of all system changes	Real-time capture	Operations
Security Metrics Dashboard	Key performance indicators and incidents	Monthly reporting	CTO
Vulnerability Reports	Current vulnerability status	Weekly production	IT Operations
Access Control Matrix	System access rights	Real-time maintenance	COO
Penetration Test Reports	External security testing results	Quarterly testing	IT Operations
Recovery Test Results	Disaster recovery and business continuity test outcomes	Per test execution	COO

STANDARD 13: CLIENT DUE DILIGENCE

Firms must conduct robust investor due diligence. This includes investor verification and due diligence procedures appropriate to regulatory requirements; risk-based approach to customer due diligence with enhanced procedures for high-risk investors; and ongoing monitoring of investor activities and transactions for suspicious activity. Firms must establish suspicious activity detection and reporting mechanisms in compliance with applicable regulations and provide regular training and testing of AML/KYC procedures for all relevant personnel.

Investor onboarding and Anti-Money Laundering (AML) processes in the digital asset sector face a unique "anonymity vs. transparency" paradox. While blockchains are technically public ledgers, the use of pseudo-anonymous addresses and instant global transfers creates a high-stakes environment for verifying identities. Traditional Know Your Customer (KYC) procedures—which rely solely on static document verification—are no longer sufficient. Modern illicit actors frequently use mixers, privacy-enhancing protocols (like Zero-Knowledge Proofs), or "chain-hopping" across cross-chain bridges to hide the origin of their wealth.

Standard 13 mandates an "intelligence-first" onboarding program that bridges the gap between traditional identity and on-chain behavior. This requires firms to collect not only government-issued identification but also the investor’s whitelisted wallet addresses to serve as a baseline for future monitoring. Today, regulatory frameworks like the EU's AMLA and the US "Failure to Prevent" doctrine have shifted the burden of proof to the manager, requiring active, forensic risk assessments that classify investors based on their geographic exposure, source of wealth, and technical footprint.

Effective AML programs must evolve from a "one-time checkbox" into a continuous risk management lifecycle. Utilizing advanced blockchain analytics is essential to identify "hops" between an investor's wallet and high-risk entities or sanctioned jurisdictions. Under current global standards, firms are legally obligated to file Suspicious Activity Reports (SARs) immediately upon detecting anomalous patterns, such as sudden "layering" or interaction with suspicious smart contracts. Institutional excellence is defined by this proactive stance—investing in specialized forensic tools and independent audits to maintain a transparent and defensible compliance posture.

13.1 INVESTOR ONBOARDING AND KYC

The investor onboarding process is the critical first touchpoint for establishing a compliant relationship. For digital asset managers, this process must be frictionless yet rigorous, bridging the gap between traditional identity verification and on-chain accountability. Unlike traditional finance, where custodial intermediaries often silo investor data, digital asset onboarding requires the direct identification of on-chain wallets to enable continuous transaction monitoring.

13.1.1 CUSTOMER IDENTIFICATION PROGRAM (CIP)

A formal CIP, updated to meet the FinCEN 2026 AML Rule requirements, must outline the mandatory steps for verifying an investor's identity.

- *For Individuals:* Collection of full legal name, date of birth, and residential address (verified via utility bills or bank statements). Valid government-issued identification (e.g., Passport, SSN, or National ID) is mandatory. Firms must also document the Source of Wealth (SoW) and verify Accredited Investor status where applicable.
- *For Entities:* Verification of legal name, jurisdiction of formation, and principal place of business. Crucially, the program must identify all Beneficial Owners with 25% or more ownership and designate a "Control Person." Source of funds must be traced to a regulated financial institution.

Verification Methodology: Firms should employ a multi-layered approach combining Documentary verification (physical ID review) with Non-Documentary methods (searching third-party databases, credit bureaus, and public records) to mitigate the risk of synthetic identity fraud.

13.1.2 ON-CHAIN KYC

Beyond traditional paperwork, institutional-grade onboarding in 2026 requires linking a verified identity to specific blockchain addresses.

- *Wallet Address Collection:* Investors must disclose all wallet addresses intended for interactions with the fund, including those used for deposits, withdrawals, and DeFi participation.
- *Proof of Address Control:* To prevent "identity piggybacking," firms must require Proof of Ownership. This is typically achieved through:

    - Signed Messages: The investor uses their private key to sign a unique, firm-provided string (e.g., "I own this wallet for Fund X on Dec 15, 2025"), proving control without exposing the key.
    - Micro-transactions*:* A "Satoshi-test" where the investor sends a specific, tiny amount of capital to a designated address.
- *Address Screening:* Every declared address is instantly screened using blockchain analytics (e.g., Chainalysis) for historical links to sanctioned entities, mixers, or darknet markets.
- *Ongoing Monitoring (KYT):* Once onboarded, these addresses enter a Know Your Transaction (KYT) workflow. Automated alerts are triggered if an investor's wallet interacts with high-risk protocols or sanctioned "smart contracts" post-onboarding.

> Many managers mistakenly treat KYC (Know Your Customer) as a one-time check. In reality, KYC is an ongoing process that requires regular updates and continuous monitoring. As investor risk profiles change—such as sources of wealth, business activities, or transaction patterns—it's important to keep KYC information current. Investment managers should ensure thorough onboarding by collecting identity verification documents, verifying wallet addresses on-chain, scheduling periodic KYC reviews, and tracking completion. For high-risk investors, enhanced due diligence is necessary, which may include additional checks and information collection. During reviews, ask questions like: '*Describe your recent high-risk investor onboarding. What extra steps were taken, and what information was gathered?*' If an investor cannot clearly distinguish between standard and high-risk onboarding or cannot provide specific examples, it indicates a weak risk management approach.

13.2 ANTI-MONEY LAUNDERING (AML) PROGRAM

An AML program consists of the internal policies, procedures, and controls designed to prevent a firm from being utilized for money laundering or terrorist financing. Institutional best practice dictates that digital asset managers maintain a formal, voluntary AML program that aligns with Bank Secrecy Act (BSA) standards. The success of such a program depends on a Risk-Based Approach (RBA)—customizing controls to address the unique threat profile of decentralized finance (DeFi) rather than relying on generic, traditional finance rules.

13.2.1 KEY COMPONENTS OF AN AML PROGRAM

A robust AML program in the current regulatory environment is built on five core "pillars" of compliance:

1. *Designated AML Compliance Officer:* A qualified individual with sufficient authority and direct access to the Board. This officer is responsible for day-to-day oversight and must possess specific expertise in blockchain-based financial crime typologies.
2. *Written AML Policy:* A Board-approved, annually reviewed document that outlines the firm's specific risk-based procedures. It must be updated to reflect recent 2026 regulatory changes, such as the Digital Asset Banking Act.
3. *Ongoing Employee Training:* Annual (minimum) training for all staff on identifying "red flags" specific to crypto, such as rapid multi-exchange movement of funds or the use of anonymity-enhancing technologies (AECs).
4. *Independent Testing:* A risk-based audit conducted annually by a qualified third party. The audit tests the effectiveness of the firm's controls, and results must be reported directly to senior management and the Board.
5. *Customer Due Diligence (CDD):* A systematic process for identifying and verifying investors, with Enhanced Due Diligence (EDD) reserved for high-risk categories like Politically Exposed Persons (PEPs) or investors from jurisdictions with weak AML oversight.

13.2.2 RISK ASSESSMENT

A formal AML risk assessment remains the foundation for any firm managing digital assets, identifying specific vulnerabilities:

- *Product Risks:* Assessing the risks of specific investment strategies, DeFi protocol participation, and redemption timeframes.
- *Customer Risks:* Evaluating investor types, geographic distribution, and the presence of complex entity structures that could obscure beneficial ownership.
- *Geographic Risks*: Monitoring transactions involving jurisdictions with weak AML regimes or those subject to active sanctions.
- *Distribution Risks*: Analyzing risks associated with direct onboarding versus the use of intermediaries or placement agents.

Many investment managers make the common mistake of using a generic AML (Anti-Money Laundering) policy without customizing it to their specific business risks. An effective AML program should be based on a thorough understanding of the actual risks the firm faces, rather than just following standard compliance rules. Generic policies often overlook unique crypto-related risks, such as the use of mixers, interactions with decentralized finance (DeFi) protocols, or cross-chain transfers. To evaluate if an AML program is properly tailored, investors typically ask for a formal risk assessment that identifies the specific risks, an AML policy that includes crypto-specific measures, examples of enhanced due diligence procedures for high-risk situations, and independent testing results with findings and corrective actions. During due diligence, a key question is: "*Can you walk us through your AML risk assessment? What are your main risks, and how does your program address them?*" If responses are generic and do not mention crypto-specific risks, it indicates the program may not be properly customized for the crypto environment.

13.3 TRANSACTION MONITORING

Transaction monitoring is the process of reviewing investor activity to identify unusual or suspicious patterns. This is a critical component of a functional AML program, serving as the primary mechanism for detecting illicit behavior after the initial onboarding phase. For digital asset managers, this requires a dual-track system: traditional monitoring for fiat movements ("off-chain") and specialized forensic analysis for blockchain activity ("on-chain").

13.3.1 ON-CHAIN AND OFF-CHAIN MONITORING

A comprehensive monitoring framework must integrate both legacy financial data and real-time blockchain telemetry to provide a 360-degree view of investor risk.

- **Off-Chain Monitoring (Traditional):** Focuses on fiat deposits and withdrawals to detect traditional money laundering typologies.
    - Anomalous Patterns: Sudden spikes in transaction frequency or sizes that are inconsistent with the investor's declared profile.
    - Structuring: Identifying multiple small transactions designed to remain just below reporting thresholds (e.g., $10,000).
    - Geographic Risk: Flagging movements involving high-risk or non-cooperative jurisdictions.

- **On-Chain Monitoring (Crypto-Specific):** Utilizes blockchain analytics tools to trace the flow of digital assets.
    - Direct & Indirect Exposure: Identifying if an investor's wallet has interacted with sanctioned addresses (e.g., the OFAC SDN list) or darknet marketplaces.
    - Anonymity-Enhancing Tools: Monitoring for the use of mixers, tumblers, or privacy protocols (e.g., Tornado Cash) that obscure the transaction trail.
    - Protocol Risks: Highlighting interactions with unregulated exchanges or high-risk DeFi protocols known for money laundering vulnerabilities.
    - Bridge Activity: Tracking assets moving across cross-chain bridges, which are frequently used by illicit actors to break the "chain of custody".

13.3.2 RED FLAGS

Firms must maintain an updated list of "red flags" that trigger immediate investigation. These indicators help compliance teams distinguish between legitimate volatile market activity and potential financial crime.

- Transactions with no apparent economic purpose or investment rationale
- Individuals or entities in high-risk jurisdictions without reasonable explanation
- Sudden unexplained increases in transaction size or frequency
- Transactions with known or suspected illicit actors identified through blockchain analytics
- Unusual transaction patterns inconsistent with stated investment objectives
- Reluctance providing requested information or documentation
- Complex ownership structures without legitimate business purpose
- Rapid movement of funds through account without investment activity

Source of funds verification for crypto-origin wealth requires capabilities beyond traditional KYC. Blockchain analytics tools can provide visibility into wallet history that investor representations alone cannot—identifying connections to high-risk activity, sanctions exposure, or mixing services that warrant additional scrutiny or rejection. Best practice is implementing blockchain analytics capability for investors whose funds originate from cryptocurrency. Wallet screening should assess transaction history, counterparty risk, and any connections to sanctioned addresses or high-risk services. The analysis should be documented and factored into the overall investor risk assessment.

13.4 SUSPICIOUS ACTIVITY REPORTING (SAR)

When a firm identifies activity that it knows, suspects, or has reason to suspect involves illicit funds or a violation of the Bank Secrecy Act, it must file a Suspicious Activity Report (SAR) with the Financial Crimes Enforcement Network (FinCEN). Filing a SAR is a mandatory legal obligation, not a discretionary choice. Any hesitation or failure to file can result in severe regulatory enforcement actions, including significant fines and potential criminal liability for the firm and its officers.

13.4.1 SAR FILING PROCESS

The filing of a SAR is subject to strict regulatory timelines and procedural requirements. A SAR must be filed within 30 calendar days from the date of initial detection of the suspicious activity. Notably, this window begins when the suspicion is first identified, not when the internal investigation is completed.

The formal process consists of the following phases:

- *Investigation:* Review the flagged behavior (e.g., unusual on-chain movements or structuring of fiat deposits) to determine if it meets the $5,000 threshold for reporting. Managers must gather all relevant transaction data, conduct internal interviews if necessary, and document the rationale for filing or not filing.
- *Preparation:* Draft a comprehensive narrative that explains the "who, what, where, when, and why" of the suspicion. The narrative must be clear, accurate, and supported by all gathered documentation. The report is submitted electronically through the FinCEN BSA E-Filing System.

- *Filing and Tracking:* Ensure the filing is submitted within the 30-day window. If the suspicious activity is ongoing, the firm must monitor the account and file supplemental SARs at least every 90 to 120 days to provide updates to law enforcement.
- *Documentation Retention:* Under federal law, firms are required to retain copies of filed SARs and all supporting documentation for a period of five years. These records must be stored securely and made available for regulatory examinations or law enforcement requests.

13.4.2 CONFIDENTIALITY

The confidentiality of a SAR is a cornerstone of the AML framework. Disclosing to the subject of a report—or to any unauthorized third party—that a SAR has been filed, or even discussed, is a direct violation of federal law. This is often referred to as "tipping off" and carries significant criminal penalties.

Strict confidentiality protocols must include:

- *Need-to-Know Access:* Access to SAR-related information must be restricted to the AML Compliance Officer and only those senior personnel necessary for the decision-making process.
- *Secure Infrastructure:* All SAR records must be maintained in a secure, encrypted environment with restricted access and immutable activity logging.
- *Prohibition on Disclosure:* SARs must never be referenced in investor reports, marketing materials, or standard financial audits.
- *Employee Training:* All staff must be trained on the legal requirement of SAR confidentiality and the severe consequences of unauthorized disclosure.
- *Law Enforcement Cooperation:* While strictly confidential, information can and should be shared with appropriate law enforcement agencies when authorized or upon receipt of a subpoena.

Sanctions compliance in digital assets extends beyond traditional name screening to include wallet address monitoring. Investors may transact with wallets that later appear on sanctions lists, or counterparties may be added to sanctions lists after relationships are established. Effective screening requires both initial and ongoing monitoring. Best practice is implementing comprehensive sanctions screening that covers: investor names and entities (against OFAC and relevant international lists), wallet addresses (against blockchain sanctions databases), and ongoing monitoring as lists are updated. Positive matches should trigger documented review and, where confirmed, appropriate action including potential relationship termination.

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional allocators evaluate AML/KYC programs by checking how well they understand their investors, identify risks, and monitor activities regularly. If they cannot clearly explain how they classify investor risks, show detailed checks for high-risk investors, or provide proof of ongoing monitoring, their compliance program may not meet industry standards.

Program Assessment

- Describe your AML/KYC framework structure and governance
- Who is your AML Officer and what is their background?
- How do you assess investor risk systematically?
- What training do you provide and how is effectiveness measured?
- How often do you test your program and what were recent findings?

Onboarding Process

- Walk through your investor onboarding process step-by-step
- How do you verify cryptocurrency-derived wealth specifically?
- What factors cause enhanced due diligence to be triggered?
- What is typical onboarding timeline for different risk levels?
- Show example documentation demonstrating thoroughness

Monitoring Capabilities

- How do you monitor investors on an ongoing basis?

- What systems and tools do you use for monitoring?
- How often do you refresh KYC information?
- What triggers immediate investor review outside normal cycle?
- Show monitoring reports and alert investigation documentation

Regulatory Compliance

- Have you filed any Suspicious Activity Reports and how many?
- Have you experienced any regulatory examinations or findings?
- How do you stay current with evolving requirements?
- What outside advisors or service providers support your program?
- Have you identified any compliance issues and how were they remediated?

Documentary Evidence Requirements

- Complete AML/KYC policies and procedures manual
- Sample investor files demonstrating process (appropriately redacted)
- Risk assessment documentation with methodology
- Staff training records with completion tracking
- Independent audit reports on program effectiveness

COMMON PITFALLS AND REMEDIATION

- *KYC treated as onboarding exercise only. Client* verified at relationship inception but never reassessed. Circumstances change—beneficial ownership evolves, transaction patterns shift, sanctions lists update—but client risk profile remains frozen at onboarding. Remediation: Implement risk-based KYC refresh: annual review for standard-risk clients, more frequent for elevated-risk. Monitor for trigger events (significant transaction pattern change, adverse media, sanctions list updates) requiring immediate review regardless of cycle.
- *AML policy ignores digital asset realities.* Generic AML framework addresses traditional banking risks but misses crypto-specific concerns: mixer and tumbler usage, privacy coin transactions, bridge activity, DeFi protocol interactions, and wallet clustering patterns. Remediation: Customize AML policies for digital assets. Define crypto-specific red flags: mixer interactions, rapid movement

through multiple wallets, privacy coin conversion, sanctioned address proximity. Train staff to recognize patterns traditional AML wouldn't flag.

- *No blockchain analytics capability*. Transaction monitoring limited to exchange reports without visibility into on-chain activity. Can't identify mixer usage, sanctioned address interactions, or suspicious wallet patterns because the data isn't being analyzed. Remediation: Deploy blockchain analytics platform with address clustering, risk scoring, and sanctions screening capabilities. Integrate outputs into client monitoring and transaction surveillance. Train compliance staff to interpret results and investigate flagged activity.
- *Reluctance to file SARs*. Suspicious activity identified but SAR filing avoided or delayed to preserve investor relationship or avoid difficult conversations. Regulatory obligation subordinated to business considerations. Remediation: Reinforce that SAR obligations are non-negotiable—duty to the financial system supersedes client relationships. Document all SAR deliberations including decisions not to file with supporting rationale. When in doubt, file—regulators criticize under-filing, not over-filing.
- *Wallet addresses not collected or verified*. Client onboarded without capturing wallet addresses used for transactions. On-chain activity can't be monitored because the firm doesn't know which wallets belong to which clients. Remediation: Require wallet address disclosure during onboarding for any client transacting in crypto. Verify wallet control through signed message or small test transaction. Include all disclosed addresses in ongoing monitoring. Update as clients add wallets.
- *AML training is generic and infrequent*. Annual training covers traditional AML concepts but not crypto-specific red flags. Staff can't identify digital asset money laundering patterns because they haven't been taught what to look for. Remediation: Provide annual training with crypto-specific content: on-chain red flags, mixer identification, DeFi-related risks, and case studies from enforcement actions. Tailor training to role—front office, compliance, and operations face different scenarios. Test comprehension, not just attendance.
- *AML program lacks independent testing*. Program designed and self-assessed by compliance without external validation. Weaknesses persist because no independent party examines whether controls actually work. Remediation: Commission annual independent AML review by qualified third party. Scope should cover policy adequacy, control effectiveness, and sample transaction testing. Present findings to board or compliance committee. Track remediation with defined timelines and accountability.

- *Sanctions screening inconsistent or point-in-time*. Screening performed at onboarding but not refreshed as sanctions lists update. Newly designated parties or addresses not detected because screening isn't ongoing. Remediation: Implement continuous sanctions screening against OFAC and relevant international lists. Screen both client names/entities and wallet addresses. Automate rescreening when lists update. Establish immediate escalation protocol for potential matches—sanctions violations have strict liability.
- *Escalation procedures unclear or untested*. Staff uncertain how to report suspicious activity, who to notify, or what documentation is required. Hesitation and delay when suspicious activity is identified because process is unclear. Remediation: Document clear escalation procedures: what triggers escalation, who receives reports, required documentation, and response timelines. Make escalation matrix easily accessible. Test periodically through scenarios—if staff can't demonstrate the process, training and documentation need improvement.

KEY CONTROLS & DOCUMENTATION

Document Type	Purpose	Update Frequency	Ownership
AML/KYC Policy	Comprehensive program framework and requirements	Annual review	AML Officer
Onboarding Procedures	Step-by-step workflow and requirements	Semi-annual review	Operations
Risk Assessment	Money laundering and terrorist financing risk analysis	Annual review	AML Officer
CDD/EDD Procedures	Due diligence standards and triggers	Annual review	Compliance
Transaction Monitoring Scenarios	Alert rules, thresholds, and parameters	Quarterly review	AML Officer

Document Type	Purpose	Update Frequency	Ownership
SAR Procedures	Investigation and filing requirements	Annual review	AML Officer
Training Materials	Role-based content and testing	Annual updates	Human Resources/Compliance
Investor KYC Files	Complete due diligence documentation	Ongoing maintenance	Operations
Sanctions Screening Records	Daily screening results and alerts	Daily capture	Compliance
Investigation and SAR Log	Case tracking and filing documentation	Ongoing maintenance	AML Officer
Blockchain Analysis Reports	Wallet verification and transaction analysis	Per investigation	Compliance

STANDARD 14: TRANSPARENCY & COMMUNICATION

Firms must maintain transparent investor relations. This includes regular and timely reporting to investors consistent with fund documents and investor expectations; clear communication of investment strategy, portfolio positioning, and material risks to investors; and transparent disclosure of fees, expenses, and conflicts of interest in offering documents and investor communications. Firms must maintain multiple channels for investor inquiries and feedback with appropriate response time commitments and establish crisis communication procedures for adverse events including operational incidents and material losses.

Transparency in digital asset management is essential to reduce information gaps. It helps investors understand operational details, custody arrangements, and potential risks. Market fluctuations make clear communication important, especially when explaining what influences performance, so investors do not misinterpret results. Custody setups involving multiple exchanges, custodians, and wallet types need clear documentation. This allows investors to assess actual risks accurately. When strategies involve DeFi protocols, derivatives, or cross-chain activities, full disclosure is necessary to prevent misunderstandings about what the firm does versus what investors might assume.

Standard 14 emphasizes the necessity of maintaining open, honest, and frequent dialogue. This includes establishing formal communication channels for rapid updates during market disruptions and providing detailed performance reports that go beyond the "what" of returns to explain the "why" of the underlying risks. Additionally, maintaining a "live" crisis communication plan ensures that during technical disruptions or protocol exploits, the firm can provide immediate, accurate information to safeguard investor confidence.

Firms adhering to this standard avoid the trap of "selective transparency" or cherry-picking reporting periods. They view operational due diligence as a partnership opportunity to demonstrate their institutional maturity rather than a burden to be minimized. Proactive disclosure—particularly regarding operational shifts or technical challenges—is favored over reactive damage control. Ultimately, admitting mistakes or strategy headwinds is seen as a necessary step in maintaining long-term fiduciary trust. Conversely, firms that avoid transparency or provide incomplete disclosures during due diligence are increasingly excluded from institutional mandates as allocators identify these behaviors as red flags for deeper operational or cultural weaknesses.

14.1 COMMUNICATION FRAMEWORK AND PHILOSOPHY

A formal communication framework provides a structured approach to engaging with investors and stakeholders. It is rooted in the principles of transparency, timeliness, clarity, and consistency. In the digital asset space, where technical complexity and market volatility are high, this framework is the primary tool for closing the "information gap" and ensuring that allocators have a clear, documented understanding of a fund's operations and risks.

14.1.1 COMMUNICATION PHILOSOPHY

The philosophy of a digital asset manager should favor radical transparency and institutional rigor. Because digital assets are often misunderstood, the manager's goal is to act as a clear translator between on-chain complexity and traditional investment standards.

- *Transparency:* A commitment to providing an unvarnished view of the fund. This includes disclosing both favorable and unfavorable events, such as protocol exploits, "de-pegging" incidents, or sudden changes in exchange counterparty risk.
- *Timeliness:* In 24/7 markets, "stale" information is a risk in itself. Managers must commit to rapid responses during periods of market stress and maintain a regular cadence of updates that investors can rely on for their own internal reporting.
- *Clarity:* The use of plain language is essential. Technical jargon (e.g., "impermanent loss," "reentrancy," or "MEV") should be clearly defined with analogies that align with traditional financial concepts to ensure the message is accessible to all levels of investor sophistication.
- *Consistency:* Maintaining a unified narrative across all channels. Whether it is a monthly performance snapshot or a direct conversation with the CIO, the data points and strategic outlook must remain aligned to prevent confusion and build long-term credibility.

14.1.2 COMMUNICATION CHANNELS

Firms should utilize a multi-channel approach to ensure that critical information reaches investors through their preferred medium while maintaining a secure "system of record."

- **Structured Reporting Cadence:**
    - *Quarterly Investor Letters:* These serve as the comprehensive "deep dive." They should include a detailed analysis of the market environment,

performance attribution (explaining *why* returns were generated), and a forward-looking discussion of portfolio positioning.

- *Monthly Updates:* A high-level performance snapshot designed for quick consumption. These updates focus on material changes in portfolio risk, current AUM, and brief commentary on significant market developments during the month.

- **Interactive & Digital Engagement:**
  - *Webinars and Conference Calls:* These provide an opportunity for live Q&A with the investment team. Annual general meetings (AGMs) or emergency "crisis calls" during extreme market events are vital for maintaining investor confidence.
  - *Secure Investor Portal:* A centralized, encrypted repository for all fund documentation. The portal should house everything from historical K-1s and monthly factsheets to educational "white papers" and the firm's latest SOC 2 security audit.

> Investor reporting that emphasizes favorable information while minimizing challenges provides incomplete transparency. Effective reporting presents a balanced view—performance in context, risks currently elevated, operational developments whether positive or negative—enabling investors to make informed assessments. Best practice is establishing reporting templates that consistently cover: performance versus benchmark and expectations, risk exposures and any elevated concerns, portfolio positioning and changes, operational developments, and outlook. The same template used in strong periods should be used in weak periods, ensuring consistent transparency rather than selective disclosure.

14.2 PERFORMANCE REPORTING STANDARDS

Performance reports are an important way to communicate with investors. These reports should be easy to understand, accurate, and transparent. They should clearly explain how the fund has performed, including the returns and the risks involved in achieving those returns. The goal is to help investors understand the fund's results without confusion, making the information straightforward and accessible for digital asset managers and investment professionals.

14.2.1 KEY COMPONENTS OF A PERFORMANCE REPORT

To ensure a report is "investor-ready," it must include standardized metrics that allow for direct comparison across different managers and asset classes.

- *Net-of-Fee Returns:* Returns must be presented after the deduction of management and performance fees to reflect the actual investor experience. Reports should clearly distinguish between Gross (reflecting investment skill) and Net (reflecting investor reality) figures across monthly, quarterly, and since-inception periods.
- *Performance Attribution:* This section identifies the "alpha" drivers. It should decompose returns by token selection, sector allocation (e.g., Layer 1s vs. DeFi), and strategy impact (e.g., yield from staking vs. spot appreciation).
- *Risk Metrics:* Given the high volatility of digital assets, risk metrics are as important as return figures.
    - Maximum Drawdown: The peak-to-trough decline, essential for understanding capital preservation.
    - Sharpe & Sortino Ratios: Measures of risk-adjusted return, helping investors determine if the volatility was "worth it."
    - Correlation: How the fund moves in relation to Bitcoin, Ethereum, and traditional benchmarks like the S&P 500.
- *Narrative Explanation:* A concise summary that provides context. It should explain how specific market events—such as protocol upgrades, regulatory shifts, or liquidity crunches—impacted the portfolio and what lessons were applied to future positioning.
- *Portfolio Composition:* A snapshot of current exposures, including top holdings, sector weightings, and the liquidity profile of the underlying assets.

14.2.2 GIPS COMPLIANCE

As discussed in Standard 10, The Global Investment Performance Standards (GIPS) are a set of voluntary, ethical guidelines for calculating and presenting investment performance. While historically focused on traditional finance, GIPS compliance has become a "strategic advantage" for digital asset managers seeking institutional capital.

To claim compliance, a firm should:

1. *Establish Policies:* Create documented procedures for calculating returns and constructing "composites" (groups of similar strategies).
2. *Avoid "Cherry-Picking":* Ensure that all fee-paying, discretionary accounts are included in at least one composite, preventing firms from only showing their most successful portfolios.
3. *Independent Verification:* Engage a third-party verifier (such as a Big Four firm or a specialist GIPS verification agency) to perform an annual audit of the firm's policies and performance presentations.
4. *Adhere to 2026 Guidance:* Incorporate recent GIPS guidance regarding fee transparency and the presentation of extracted performance (e.g., individual case studies) alongside the total portfolio results.

> In performance reporting, a common mistake is missing important context. Managers might show high returns but not mention the risks they took or favorable market conditions that helped achieve those results. Looking at return alone gives an incomplete picture. To properly evaluate a manager's skill, it is important to understand the risks involved, the strategies used, and the market environment during the period. Investors and analysts assess the quality of performance reports by asking for: (a) Complete performance history across all periods, (b) Attribution analysis to explain where returns came from, (c) Risk metrics to provide context on volatility and risk taken, and (d) Benchmark comparisons with tracking error analysis. During due diligence, a common question is: "*Describe your worst performing period. What happened, what did you learn, and what changes did you make afterward?*" Managers who avoid discussing mistakes or blame external factors may be hiding a lack of self-assessment or reluctance to admit errors. Clear, honest responses help assess the manager's ability to learn and adapt, which is crucial in the investment industry, especially for digital asset managers.

14.3 OPERATIONAL TRANSPARENCY

Operational transparency allows investors to verify how a firm executes its strategy and manages risk. For institutional allocators, operational failures are often seen as more significant than investment losses, as they represent a failure of the firm's core governance. Clear,

straightforward communication about internal processes is essential for building a "partnership of trust" with institutional clients.

14.3.1 DUE DILIGENCE QUESTIONNAIRE (DDQ)

A Due Diligence Questionnaire (DDQ) acts as an "MRI scan" of your entire organization. It should provide a standardized, transparent overview of your strategy, technology, and risk controls. For digital asset managers, the DDQ must bridge the gap between complex blockchain mechanics and institutional expectations.

Key Attributes of an Institutional DDQ:

- *Comprehensive Coverage:* The document must address the full operational spectrum, including organizational structure, investment process, risk management, compliance, cybersecurity, and specific custody arrangements.
- *Current and Dynamic:* The DDQ should be updated at least annually or immediately following a "material change" (e.g., a change in lead custodian or a shift in the AML compliance officer).
- *Specific and Quantitative:* Managers should avoid generic responses. Provide data on historical uptime, average withdrawal processing times, and third-party audit results.
- *Radical Honesty:* Transparently disclose past operational challenges or limitations. Acknowledging areas for improvement and detailing the remediation steps taken builds more credibility than attempting to obscure flaws.

14.3.2 OPERATIONAL DUE DILIGENCE (ODD)

Institutional allocators conduct rigorous ODD reviews to ensure that a firm's stated policies match its actual daily practices. This process often involves deep-dive interviews and on-site (or virtual) system demonstrations.

Preparation Strategy:

- *Documentation Readiness:* All internal policies—specifically your Incident Response Plan, Business Continuity Plan (BCP), and Valuation Policy—must be organized and ready for immediate review.
- *Personnel Access:* Ensure that key operational leads (COO, CISO, AML Officer) are available to discuss their specific domains. They should be briefed to provide consistent, technical, and transparent answers.
- *Systems Walkthrough:* Be prepared to demonstrate your technology in action. This may include showing how a transaction is authorized via a multi-signature

wallet, how risk limits are monitored in real-time, or how the firm reconciles on-chain balances with its internal ledger.

- *Partnership Mindset:* View the ODD process as a collaborative exercise. Welcoming scrutiny and responding constructively to "gaps" identified by the allocator demonstrates a culture of continuous improvement, which is highly valued by long-term partners.

Common mistakes during ODD (Operational Due Diligence) reviews include being defensive or evasive. Good managers see ODD as an opportunity to show operational strength and are open to scrutiny. Responding defensively to legitimate questions raises concerns about what the firm might be hiding. Evasive answers can indicate a lack of documentation or a reluctance to admit weaknesses. During ODD, evaluators look for how well the firm responds to requests for information, how honest it is about challenges, its willingness to provide supporting documents, and how it handles concerns. The most damaging behaviors are refusing to share requested documents, giving inconsistent answers, failing to prove controls are effective, or showing hostility when questioned. These behaviors suggest operational issues or cultural problems that could disqualify the firm from gaining institutional capital.

14.4 EDUCATIONAL CONTENT AND THOUGHT LEADERSHIP

In the rapidly evolving digital asset landscape, education is a cornerstone of investor relations. Because blockchain technology and market structures are inherently complex, providing high-quality educational content helps investors contextualize volatility and technical risks. This proactive approach leads to more realistic investor expectations and stabilizes capital flows during periods of market stress.

14.4.1 EDUCATIONAL CONTENT

Investment managers specializing in digital assets should create different types of educational materials. These materials help clients understand digital assets and how to manage them effectively. Examples include articles, videos, webinars, and guides. Providing clear and simple information is essential to ensure clients can easily grasp complex concepts related to digital assets:

- *White Papers:* These represent the "gold standard" of deep-dive analysis. They should provide rigorous, data-backed examinations of protocol upgrades (e.g., Ethereum's transition to "Dencun" or the impact of "Proto-Danksharding"), market structure shifts, or evolving regulatory landscapes like the MiCA framework.
- *Webinars and Training Sessions:* Live or recorded sessions that demystify complex topics—such as liquid staking, yield farming risks, or MEV (Maximum Extractable Value) mechanics—allow for direct interaction and Q&A, humanizing the technical expertise of the firm.
- *Glossaries and FAQs:* Standardizing terminology is vital. A central repository explaining terms like "cold storage," "MPC," "slippage," and "gas fees" helps prevent fundamental misunderstandings during operational reviews.
- *Multi-Format Strategy:* Information should be repurposed across blog posts, LinkedIn "explainers," and short-form videos to reach investors through their preferred consumption channels.

14.4.2 THOUGHT LEADERSHIP

Thought leadership moves beyond general education to offer unique, valuable, and often contrarian perspectives that build long-term credibility.

- *Original Perspective:* Rather than merely summarizing news, effective thought leadership uses proprietary research and data to offer a "house view" on the future of the industry.
- *Intellectual Honesty:* Credibility is maintained by acknowledging the limitations of current technology and being objective about the risks of specific strategies. Admitting when a previous thesis was incorrect is often more valuable for building trust than constant self-promotion.
- *Objectivity:* Research should remain balanced. For instance, an analysis of a new Layer 2 protocol should discuss its throughput benefits alongside its potential centralization risks or bridge vulnerabilities.

14.5 CRISIS COMMUNICATION AND INCIDENT RESPONSE

A crisis communication plan is a formal guide that explains how a company communicates with investors and stakeholders during major problems. These problems can include cyber-attacks, regulatory issues, key staff leaving, performance problems, or operational failures.

How a company communicates during a crisis is often more important for maintaining long-term trust than the crisis itself.

14.5.1 CRISIS COMMUNICATION PLAN

A comprehensive plan must be pre-approved by the Board and the legal team to minimize decision-making lag during an actual emergency.

- *Crisis Response Team:* A small, cross-functional group (typically 3–5 people) including the CEO, CISO, and Legal Counsel. This team has the authority to approve statements and make rapid decisions.
- *Pre-Approved Templates:* Developing "holding statements" for common scenarios (e.g., a service provider outage or a suspected wallet compromise) allows the firm to communicate within the first 15–30 minutes of an event.
- *Designated Spokespeople:* To prevent contradictory messages, all external communication must flow through pre-identified spokespeople who have undergone specific crisis media training.

14.5.2 INCIDENT RESPONSE COMMUNICATION

Communication is the final step in the technical incident response cycle. It should follow a disciplined "Before-During-After" cadence:

1. *Initial Notification (The "First Hour"):* Rapidly acknowledge the incident. Provide only verified facts, state that an investigation is underway, and specify when the next update will be provided.
2. *Investigation Updates:* Provide regular status reports (e.g., every 60 minutes during a critical system outage) even if no new facts are available. This prevents the spread of rumors on social platforms.
3. *Resolution & Post-Mortem:* Once resolved, provide a detailed "Root Cause Analysis" (RCA). This should explain what happened, how the firm responded, and the specific technical or operational changes implemented to prevent a recurrence.
4. *Feedback Loop:* After the crisis, review the effectiveness of the communication efforts with key investors to refine the plan for future resilience.

Crisis communication quality often determines whether investors remain supportive during difficulties or immediately redeem. Rapid transparent communication builds trust even when delivering bad news. Delayed evasive communication destroys trust regardless of ultimate resolution. Allocators assess crisis preparedness by requesting: crisis communication plan documentation, examples of past incident communications, post-incident reviews with lessons learned, crisis communication testing or tabletop exercise results. Inability to acknowledge difficult situations or defensive responses about communication choices reveal either lack of experience or unwillingness learning from mistakes—both concerning for future crisis management.

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional allocators evaluate transparency through communication quality, reporting completeness, and operational due diligence responsiveness. Inability to provide comprehensive DDQs, produce sample communications demonstrating transparency, or explain crisis communication procedures reveals inadequate investor relations infrastructure.

Communication Framework and Reporting

- Walk through your investor communication framework—what regular communications occur and what triggers ad-hoc updates?
- Show representative sample monthly and quarterly investor reports. What specific risk and performance metrics do you consistently provide?
- How do you handle reporting during difficult performance periods? Selective reporting or lack of context during drawdowns signals inadequate transparency.
- Are you GIPS compliant? If not, what performance standards do you follow and why?

Operational Transparency

- Provide your current DDQ. Outdated DDQs or resistance to providing them indicates inadequate maintenance or reluctance to disclose operational details.
- Walk through your approach to operational due diligence—how quickly do you respond to requests and what level of detail do you provide?
- What operational details do you share with investors and how can investors independently verify information you provide?

- What information and functionality does your investor portal provide?

Investor Education

- What educational content do you provide to help investors understand your strategy and digital asset concepts?
- How do you explain complex digital asset concepts to traditional allocators?
- Show examples of educational materials at different sophistication levels.

Crisis Communication

- Walk through your crisis communication plan—what triggers immediate notification and what are response timeframes?
- How quickly do you commit to notifying investors of material events?
- Provide an example of how you handled adverse event communication. Inability to provide specific example suggests either perfect track record (unlikely) or inadequate transparency when problems occur.

Documentary Evidence Requirements

- Investor communication policy with cadence and content standards
- Complete set of recent monthly performance letters and quarterly operational reports
- Current DDQ updated within past quarter
- Performance reporting showing GIPS compliance or alternative standards
- Educational materials demonstrating range and quality
- Crisis communication plan with notification triggers and tested procedures
- Investor portal demonstration with functionality

COMMON PITFALLS & REMEDIATION

- *Performance presented selectively*. Marketing materials highlight favorable periods while omitting drawdowns or underperformance. Investors presented with incomplete picture can't assess true track record or manager skill versus market conditions. Remediation: Present complete performance from inception through current period—no gaps, no cherry-picked windows. Provide context for both strong and weak periods: what drove results, how risk was managed,

what was learned. Apply GIPS standards or equivalent methodology for credibility.

- *Defensive posture during operational due diligence*. ODD requests treated as adversarial interrogation rather than legitimate investor need. Responses are guarded, documentation slow to produce, and tone suggests firm has something to hide—even when it doesn't. Remediation: Approach ODD as partnership opportunity demonstrating operational quality. Maintain organized documentation ready for common requests. Respond promptly and completely. If weaknesses exist, acknowledge them with remediation plans rather than deflecting—allocators respect transparency more than perfection.
- *DDQ responses generic and templated*. Questionnaire answers are vague, clearly copied from templates, or don't address the specific question asked. Suggests either weak operations or lack of attention to the investor relationship. Remediation: Provide specific, detailed responses with concrete examples and documentation references. Customize answers to each DDQ rather than pasting standard language. Update responses as operations evolve—stale DDQs signal inattention. Review responses for accuracy before submission.
- *Crisis communication slow or absent*. During incidents, firm goes silent while investors learn details from news or social media. Delayed communication amplifies anxiety and damages trust more than the underlying incident. Remediation: Communicate promptly when material incidents occur—acknowledge the situation even before full details are known. Provide regular updates as investigation progresses. Be transparent about what happened, impact assessment, and remediation steps. Silence is never the right strategy.
- *Investor communication is one-directional*. Reports distributed but no mechanism for investor questions, feedback, or dialogue. Investors feel like passive recipients rather than partners whose concerns matter. Remediation: Create opportunities for two-way engagement: quarterly Q&A calls, annual investor meetings, accessible investor relations contact. Solicit feedback on reporting quality and responsiveness. Document investor concerns and demonstrate responsiveness through visible action on legitimate issues.
- *Performance reporting lacks risk context*. Returns presented without attribution, risk metrics, or market context. Investors can't distinguish skill from beta, or understand whether returns were achieved with appropriate or excessive risk. Remediation: Include risk-adjusted metrics (Sharpe ratio, drawdown analysis), performance attribution explaining return drivers, and market context for the period. Explain both what went right and what went wrong. Reporting that only celebrates gains without acknowledging risks lacks credibility.

- *No crisis communication plan*. Incident occurs and firm improvises response—who communicates, what message, which investors first, how to handle media. Confusion and inconsistency make situation worse. Remediation: Document crisis communication plan covering: incident classification, escalation matrix, spokesperson designation, message approval process, investor notification sequence, and media protocol. Test through tabletop exercises annually. Update contact information quarterly—a plan with wrong numbers is useless.
- *Disclosure practices inconsistent*. Material information shared with some investors but not others, or disclosed reactively when discovered rather than proactively when known. Ad hoc approach creates fairness concerns and legal exposure. Remediation: Establish disclosure policy defining: what constitutes material information requiring disclosure, timing requirements, approval process, and distribution method ensuring all investors receive information simultaneously. Document disclosure decisions including rationale for materiality determinations.
- *Governance structure opaque to investors*. Investors can't determine who oversees the firm, what independent oversight exists, or how key decisions are made. Lack of transparency suggests governance may be weak or non-existent. Remediation: Publish governance summary covering: board composition and independence, committee structure and responsibilities, key personnel roles, and oversight mechanisms. Make available during ODD and include summary in investor materials. Transparency about governance demonstrates institutional maturity.

KEY CONTROLS & DOCUMENTATION

Document Type	Purpose	Update Frequency	Ownership
Communication Policy	Overall framework and standards governing all communications	Annual review	Chief Executive Officer (CEO)/Chief Compliance Officer (CCO)

Document Type	Purpose	Update Frequency	Ownership
Reporting Calendar	Master schedule for all reporting obligations and distributions	Annual planning with monthly updates	Chief Operating Officer (COO)
Performance Report Templates	Standardized formats ensuring consistency and completeness	Quarterly review and enhancement	Chief Financial Officer (CFO)
Crisis Communication Plan	Emergency response procedures and protocols	Semi-annual review and testing	CEO
Content Calendar	Planned educational materials and thought leadership	Quarterly planning with weekly execution	Marketing/Communications
Investor Portal Documentation	Portal functionality, data sources, and access controls	Monthly updates as changes occur	Technology/Operations
Media and Social Media Policy	Guidelines for external communications and social engagement	Annual review or as needed	Compliance/Marketing
Disclosure Matrix	Disclosure requirements by audience and situation	Quarterly review	CCO
Investor Feedback Log	Record of questions, concerns, and responses	Ongoing maintenance	Investor Relations
Communication Metrics Dashboard	Engagement and effectiveness measurements	Monthly reporting	Marketing/Communications
Incident Communication Log	Record of all crisis communications and outcomes	Ongoing maintenance	Compliance

Document Type	Purpose	Update Frequency	Ownership
Content Library	Repository of all approved materials and versions	Ongoing maintenance	Marketing
Regulatory Filing Schedule	All regulatory deadlines and requirements	Quarterly review	Compliance

STANDARD 15: ORGANIZATIONAL CONTINUITY

Firms must ensure organizational resilience. This includes identification and mitigation of key person dependencies through cross-training and knowledge documentation; professional development programs and succession planning for critical roles; and competitive compensation and retention strategies appropriate to market and firm size. Firms must provide regular training on compliance, risk management, and operational procedures and document critical processes and institutional knowledge to ensure continuity.

Institutional resilience in digital asset management is fundamentally tied to the strength and stability of its human capital. Standard 15 requires firms to mitigate "key person risk" through a structured framework of cross-training, knowledge documentation, and succession planning. In an industry where specialized technical expertise and critical counterparty relationships are often concentrated in a few individuals, firms must treat organizational depth as a core risk management function. This includes implementing professional development programs and competitive retention strategies that are calibrated to both market standards and the firm's specific operational scale.

The digital asset sector faces uniquely high human capital risks due to its relative infancy and the highly specialized nature of the talent pool. Founders and lead engineers often possess "siloed" technical knowledge—such as private key management protocols or proprietary trading algorithms—that is difficult to replace quickly. Historical data from the broader hedge fund industry demonstrates that while some firms successfully transition talent, many fail when their success is overly dependent on specific individuals rather than institutionalized infrastructure. For digital asset managers, the complexity of the technology and the lack of a deep, seasoned labor market make the loss of a key employee a potential threat to the firm's survival.

To satisfy Standard 15, firms must transition from a "founder-centric" model to an institutionalized structure where resilience is built into the workflow. This involves identifying "single points of failure" within the team and creating documented succession plans with designated, trained alternates for every critical role. Essential operational processes must be recorded in an institutional knowledge base to ensure continuity during personnel shifts. While investing in team redundancy and cross-training may appear inefficient during periods of stability, it is a vital safeguard against the inevitable disruption of turnover. Institutional

allocators prioritize firms that demonstrate this organizational depth, viewing it as a prerequisite for long-term fiduciary reliability.

15.1 ORGANIZATIONAL STRUCTURE AND TALENT STRATEGY

A transparent organizational structure and a forward-thinking talent strategy are the bedrock of effective personnel management. The firm’s architecture must align with its strategic business goals, ensuring that every team member understands their role, their reporting lines, and the firm's capacity for growth. In the competitive digital asset landscape, a talent strategy must prioritize the recruitment of specialized expertise, continuous professional development, and the retention of high-performing individuals to maintain an edge.

15.1.1 ORGANIZATIONAL STRUCTURE

A formal organizational chart should serve as the definitive map of the firm's hierarchy. This structure is designed to promote oversight and operational efficiency through several key principles:

- *Segregation of Duties:* To prevent conflicts of interest and fraud, there must be a clear separation between the Investment Team, Operations, and Compliance. Investment personnel should never have unilateral control over operational or compliance functions, ensuring that a "second pair of eyes" is always present for critical movements.
- *Clear Accountability:* Every role requires a specific mandate and defined level of authority. By eliminating overlaps and gaps in responsibility, the firm ensures that every operational aspect is owned by a specific individual, with clear escalation paths for issues requiring senior intervention.
- *Scalability:* The structure should be built with growth in mind, allowing the firm to add new functions (e.g., a dedicated DeFi Research role or an Institutional Sales team) without requiring a total reorganization.
- *Reporting Efficiency:* Management should maintain an appropriate "span of control" to prevent communication bottlenecks. Critical functions should have direct lines to senior leadership, with the Board of Directors providing ultimate oversight.

15.1.2 TALENT STRATEGY

Attracting and retaining the specialized talent required for digital asset management requires a disciplined, multi-stage lifecycle approach:

- *Recruiting:* Firms must proactively identify talent through diverse channels, including specialized recruiting firms and industry networking. The interview process should be rigorous, assessing not only technical blockchain proficiency but also "cultural fit" and adherence to the firm's ethical standards.
- *Onboarding:* A structured integration process is essential. New hires should receive immediate training on the firm's specific technology stack, security protocols, and compliance culture, often supported by a mentorship assignment to accelerate their integration.
- *Training and Development:* Given the pace of technical change, ongoing education is mandatory. This includes support for continuing education, attendance at key industry conferences, and internal "knowledge-sharing" sessions to ensure the team stays current on protocol upgrades and regulatory shifts.
- *Performance Management:* Formal, merit-based evaluations should link individual goals to the firm's long-term objectives. Regular feedback loops, rather than just annual reviews, allow for real-time coaching and the identification of high-potential employees for future leadership roles.

> Many organizations make the mistake of having a complex structure that doesn't match their strategy. A simple and clear organizational setup is often more effective than complicated hierarchies, which can cause communication problems and confusion about responsibilities. The structure should support the business needs, not restrict flexibility with rigid frameworks. When evaluating an organization, assessors typically ask for the current organizational chart showing reporting lines, descriptions of key roles, explanations of how duties are separated, and recent changes with reasons. Large differences between the formal structure and actual practices can indicate either an ineffective setup or poor documentation, both of which are concerning.

15.2 KEY-PERSON RISK MANAGEMENT

Key-person risk is the danger that losing an important individual could significantly harm a company's operations. In the digital asset sector, where specialized technical knowledge and complex counterparty relationships are often concentrated within small, agile teams, this risk is acutely high. Effective management requires a shift from "hope-based" retention to a proactive framework of identification, impact assessment, and structural redundancy.

15.2.1 IDENTIFYING KEY PERSONS

The first step in mitigation is identifying individuals whose absence would create a "single point of failure." In an institutional digital asset firm, these roles typically include:

- *Founder or CEO:* Often the primary holder of strategic vision and key investor relationships. In many jurisdictions, the CEO may also hold specific regulatory authorizations that are not easily transferable.
- *Chief Investment Officer (CIO):* The architect of the investment strategy. The CIO often possesses unique market insights and proprietary decision-making frameworks that drive the fund's track record.
- *Specialized Portfolio Managers/Researchers:* Individuals with "siloed" expertise in niche areas, such as DeFi, quantitative modeling, or on-chain research.
- *Head of Operations or Technology:* The gatekeeper of critical infrastructure. This person often manages the complex relationships between the firm, its custodians, and its technology vendors.
- *Chief Compliance Officer (CCO):* The primary liaison with regulators. The CCO's deep understanding of the firm's specific compliance program and their established relationships with examiners are vital for maintaining the firm's "license to operate."

15.2.2 MITIGATING KEY-PERSON RISK

To protect the firm from the sudden departure, disability, or death of a key individual, managers must implement a multi-layered redundancy strategy:

Institutionalization of Knowledge:

- *Process Documentation:* Every critical operational task—from executing a multi-signature transaction to performing a month-end NAV reconciliation—must be documented in a step-by-step manual. This allows a trained secondary staff member to execute the task without improvisation.

- *Knowledge Management Systems:* Use collaborative platforms to capture investment theses, research notes, and meeting minutes. This ensures that "institutional memory" resides in the firm's databases rather than just in an individual's mind.

Personnel Redundancy:

- *Succession Planning:* Every key role should have a named "successor-in-waiting." These individuals should have formal development plans to bridge any skill gaps, ensuring they are ready to step in at a moment's notice.
- *Cross-Training:* Implement a mandatory cross-training program where secondary personnel regularly perform the functions of a key person under supervision. This builds "bench depth" and ensures operational continuity.

Financial and Legal Safeguards:

- *Key-Person Insurance:* The firm should maintain insurance policies that provide a financial buffer upon the death or disability of a critical leader. This capital can be used to fund a global executive search or offset temporary revenue losses.
- *Notice Periods and Non-Competes:* Ensure employment contracts include appropriate notice periods to allow for an orderly transition, alongside non-compete clauses that protect the firm's proprietary strategies and relationships.

Succession plans sitting in binders without testing fail when actually needed. Effective succession planning requires living documentation regularly reviewed and updated, named successors actively being developed for future roles, and organizations capable of executing smooth transitions when key personnel depart. Paper plans without preparation create leadership vacuums during critical transitions—exactly when firms can least afford operational disruption. Allocators evaluate succession planning by examining formal documentation identifying specific successors, development plans preparing those individuals for expanded responsibilities, cross-training programs building redundancy across critical functions, and response procedures for handling key departures. The revealing due diligence question: "*If your CIO left tomorrow, who would take over and how prepared are they? Walk us through the transition process.*" Vague responses failing to name specific successors or acknowledge transition challenges signal weak succession planning regardless of documentation existence. Sophisticated allocators recognize that succession planning quality becomes visible only during actual transitions—but by then it's too late to fix deficiencies.

15.3 TALENT ACQUISITION AND DEVELOPMENT

In competitive digital asset markets, attracting and developing top talent constitutes a key differentiator. Firms should maintain proactive strategic approaches to talent acquisition and development, recognizing that human capital quality directly determines operational excellence and competitive positioning.

15.3.1 TALENT ACQUISITION

Talent acquisition strategies for digital asset managers should focus on attracting skilled professionals who understand blockchain technology, cryptocurrencies, and digital investments. Additionally, training programs can help new hires adapt quickly and stay updated with industry trends. A straightforward and effective talent acquisition plan ensures that digital asset management firms have the right team to succeed in a competitive market:

- *Employer Brand:* Establish a clear, compelling employer value proposition. A strong reputation is essential for attracting top talent, with a mission and culture that resonates with desired candidates. Maintain a public presence through content and industry participation to secure competitive positioning in the talent market.
- *Multi-channel Sourcing:* Utilize employee referrals with incentive programs, industry networking, and relationship building. Leverage recruiting firms for specialized or senior positions, alongside social media, online platforms, and university relationships for junior talent. Participate in conferences and speaking engagements to extend reach.
- *Interview Process:* Implement a structured process assessing skills, experience, and cultural fit. Use multiple interviewers to provide diverse perspectives and technical assessments for specialized roles. Conduct rigorous reference checks and background checks for all positions, maintaining a clear timeline and consistent communication with candidates.
- *Competitive Offers*: Provide market-competitive compensation packages. This includes comprehensive benefits such as health insurance and retirement plans, as well as equity or profit-sharing opportunities. Offer flexible work arrangements where appropriate and robust professional development support.

15.3.2 TALENT DEVELOPMENT

The talent development program for digital asset managers should focus on essential skills and knowledge through the following structured components:

- *Structured Onboarding:* A comprehensive orientation covering firm culture, systems, and processes. This includes training on specific tools and platforms with clear 30-60-90 day objectives. Facilitate regular check-ins with managers and mentors to assess onboarding effectiveness.
- *Ongoing Training:* Prioritize technical skills development to keep pace with evolving markets. Provide leadership and management training for advancing personnel, and support industry certifications, designations, and external courses. Encourage internal knowledge-sharing sessions.
- *Mentorship Programs:* Pair junior employees with senior mentors for regular guidance and career development discussions. This provides exposure to senior-level decision-making and helps build professional networks both within and outside the firm.
- *Career Pathing:* Establish clear advancement criteria and timelines. Create development plans for high-potential employees and provide "stretch assignments" for growth. Support internal mobility to enable career progression and maintain a healthy succession pipeline.

> Many firms make the mistake of focusing only on hiring senior talent and ignoring the development of junior employees. Investing in the growth of junior staff helps build stronger teams and creates a better plan for future leadership. Developing talent from within the company is often more effective than always hiring externally. Internal employees already understand the company's culture and processes, which makes their transition smoother. External hires usually need more time to adapt, which can slow down progress. When evaluating a firm's talent development efforts, investors often ask for specific information. This includes the company's training budgets and programs, examples of employees who have been promoted internally, details about mentorship programs, employee retention rates based on tenure, and development plans for high-potential employees.

15.4 COMPENSATION AND RETENTION STRATEGY

A competitive compensation and retention strategy is essential for attracting and retaining top-tier talent in the digital asset sector. Compensation programs must be fair, transparent, and aligned with firm performance while incentivizing behaviors that support long-term institutional stability rather than excessive, short-term risk-taking.

15.4.1 COMPENSATION PHILOSOPHY

A compensation philosophy should be based on principles that balance market-leading rewards with rigorous accountability.

- *Pay for Performance:* A significant portion of total compensation should be variable and tied directly to both individual objectives and overall firm performance. This creates a clear differentiation between high and low performers through annual evaluations.
- *Long-Term Alignment:* To align employee interests with those of the firm and its investors, managers should utilize deferred compensation and long-term incentives (LTIs).
    - Vesting Schedules: Use structured vesting (e.g., a four-year schedule with a one-year cliff) to encourage long-term commitment.
    - Equity & Participation: Offer profit-sharing or equity stakes to turn employees into true stakeholders.
    - Clawback Provisions: Maintain formal policies to reclaim variable compensation in instances of misconduct, regulatory breaches, or significant performance reversals.
- *Market Competitiveness*: Conduct regular benchmarking studies to ensure salary and bonus ranges remain competitive within the digital asset and broader financial sectors. Adjustments should account for geographic location, cost of living, and the total value of benefits.
- *Transparency:* Clearly communicate the criteria used to determine compensation. Objective metrics help eliminate bias, while an established appeals process ensures disputes are handled fairly and professionally.

15.4.2 RETENTION STRATEGY

Retaining top talent requires more than financial rewards; it involves creating an environment where skilled managers feel intellectually challenged and professionally supported.

- *Competitive Compensation and Benefits:* Beyond high base pay and bonuses, provide comprehensive benefits including health insurance, retirement plans, and insurance coverage. High-performers should see a clear link between their success and their financial trajectory.
- *Challenging Work Environment:* Digital asset professionals are often driven by the opportunity to work with cutting-edge technologies. Provide autonomy in decision-making and assign projects that allow staff to contribute to innovative strategies and infrastructure.
- *Career Growth Opportunities:* Establish transparent advancement paths with objective criteria for promotion. Invest in continuous training, industry certifications, and leadership development to prepare internal talent for increasing levels of responsibility.
- *Strong Positive Culture:* Foster a collaborative and inclusive environment that prioritizes work-life balance and flexibility. Regular team-building activities, open feedback loops, and a visible commitment to diversity help build a loyal and engaged workforce.

Compensation structures that reward short-term performance without long-term alignment may incentivize excessive risk-taking. Variable compensation without deferrals, clawbacks, or connection to investor outcomes creates incentives misaligned with fiduciary obligations and long-term firm success. Best practice is structuring compensation with meaningful deferral periods (aligning employee holding periods with investor lock-ups where possible), clawback provisions for compliance failures or investment losses, and connection between variable compensation and investor outcomes. The structure should encourage decisions consistent with long-term investor interests, not just current-period performance.

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional allocators evaluate human capital through key person dependency, succession planning adequacy, and compensation alignment. Inability to demonstrate succession planning beyond aspirational statements or explain compensation structures aligning long-term interests reveals organizational fragility.

Organizational Structure and Key Person Risk

- Walk through your organizational structure. Provide current organizational chart with reporting relationships.
- Who are key persons whose absence would materially disrupt operations and how is each role's key person risk mitigated?
- Walk through your succession plan for each critical role—who is backup, what knowledge transfer has occurred, what testing validates capability?
- What happens operationally if your CIO is unavailable for 30 days?

Talent Strategy and Retention

- What is your talent strategy for attracting and retaining personnel in competitive digital asset labor market?
- What is your turnover rate overall and by function? What are the primary departure reasons?
- How do you develop talent internally through training, mentorship, and career progression?
- What development programs exist and how is effectiveness measured?

Compensation and Alignment

- What is your compensation philosophy and how does it balance base, bonus, and deferred compensation?
- What percentage of compensation is deferred over multiple years? Short-term structures without deferrals signal misalignment.
- How is compensation linked to individual performance, firm performance, and investor outcomes?
- Do founders have significant personal capital invested in funds?

Culture Assessment

- How do you define culture beyond generic statements? What are your specific core values with behavioral examples?
- How do you measure engagement and cultural health? Provide employee engagement survey results if conducted.
- Give concrete examples of cultural decisions during difficulties.

Documentary Evidence Requirements

- Current organizational chart with all personnel and reporting relationships
- Complete biographies for key personnel
- Key person risk assessments with mitigation plans
- Succession plans with backup coverage and knowledge transfer documentation
- Compensation policy describing structure and alignment
- Turnover statistics with analysis
- Employee engagement survey results demonstrating systematic feedback

---

COMMON PITFALLS & REMEDIATION

- *Succession plan exists on paper only.* Document names successors but designated individuals have never performed critical functions, lack necessary training, or aren't aware they're designated. Plan provides false comfort without operational readiness. Remediation: Name specific successors for each critical role. Ensure successors have actually performed key functions—not just observed or been briefed. Conduct annual transition simulations testing whether successors can execute independently. Document procedures enabling handover without the incumbent's involvement.
- *Critical knowledge concentrated in few individuals.* Key processes, relationships, or expertise exist only in the heads of one or two people. Departure, illness, or unavailability creates operational disruption or capability loss. Remediation: Document critical processes in sufficient detail for someone unfamiliar to execute. Implement cross-training ensuring at least two people can perform each essential function. Maintain knowledge repository accessible to appropriate

personnel. Regular knowledge-sharing sessions reduce single-point-of-failure risk.

- *Compensation incentivizes short-term risk-taking*. Bonuses tied to annual performance without deferrals, clawbacks, or alignment with investor outcomes. Structure encourages maximizing current-year returns regardless of risk taken or long-term consequences. Remediation: Implement meaningful deferrals (2-3 years minimum) with vesting tied to continued employment and fund performance. Include clawback provisions for compliance failures, material errors, or subsequent investment losses. Balance metrics across performance, risk management, and operational quality.
- *Junior talent development neglected*. Firm relies on external hiring for advancement, creating organization without institutional knowledge continuity or clear career paths. High performers leave for opportunities elsewhere because internal progression is blocked. Remediation: Invest in training and development programs. Establish mentorship relationships pairing junior staff with senior leaders. Define career paths showing progression opportunities. Promote from within where qualified candidates exist—external hiring for every senior role signals development failure.
- *Employee turnover unexamined*. People leave and are replaced without analyzing why departures occur or whether patterns indicate systemic issues. Problems persist because root causes aren't identified. Remediation: Conduct meaningful exit interviews—not just HR formality—probing actual reasons for departure. Analyze turnover data for patterns: specific managers, roles, tenure points, or compensation issues. Benchmark compensation and culture against competitors. Address identified issues rather than accepting turnover as inevitable.
- *Roles and accountability unclear*. Responsibilities overlap, gaps exist between functions, or reporting relationships create confusion. When problems occur, unclear who owns resolution. Accountability diffused means accountability absent. Remediation: Document clear role descriptions specifying responsibilities, decision authority, and reporting relationships. Maintain current organizational chart reflecting actual structure. Review annually and update when roles evolve—outdated documentation is worse than none because it misleads.
- *No key-person insurance*. Firm heavily dependent on founder or key individuals but lacks financial protection if they become unavailable. Death or disability of critical person creates both operational and financial crisis simultaneously. Remediation: Assess key-person risk identifying individuals whose absence would materially impact operations or investor confidence. Obtain appropriate

insurance coverage sized to bridge transition period. Review coverage annually as firm evolves and key-person dependencies shift.

- *Board doesn't oversee leadership continuity*. Succession planning delegated to management without board visibility or challenge. No regular assessment of leadership depth, development progress, or readiness for transitions. Remediation: Assign succession oversight to board or governance committee. Review succession plans and leadership development annually. Assess depth at each critical position—single-deep coverage at senior levels warrants attention. Challenge management on development progress and timeline for addressing gaps.
- *Culture transmitted informally, not reinforced systematically*. Firm values exist as implicit norms understood by long-tenured employees but not articulated, taught, or reinforced. New hires absorb culture inconsistently; values dilute as firm grows. Remediation: Articulate firm values explicitly in writing. Incorporate values into hiring criteria, onboarding, performance reviews, and promotion decisions. Assess cultural alignment periodically through surveys or conversations. Address misalignment directly—culture that isn't actively maintained erodes.

KEY CONTROLS & DOCUMENTATION

Document Type	Purpose	Update Frequency	Ownership
Organizational Chart	Current structure and reporting relationships	Monthly updates	Human Resources (HR)
Role Descriptions	Position requirements and responsibilities	Annual review	HR/Department Managers
Succession Plans	Coverage plans for all key roles	Semi-annual review	CEO/Board
Compensation Philosophy	Strategy and market positioning	Annual review	CEO/Board
Employee Handbook	Comprehensive policies and procedures	Annual review	HR/Legal

Document Type	Purpose	Update Frequency	Ownership
Performance Management Framework	Review processes and criteria	Annual review	HR
Training and Development Records	Completion tracking and compliance	Ongoing maintenance	HR
Key Person Risk Register	Critical personnel identification and backups	Quarterly review	COO
Cultural Values Documentation	Core values and behavioral expectations	Annual review	CEO
Retention Analysis	Turnover data and trend analysis	Quarterly reporting	HR
Recruitment Pipeline Tracking	Candidate sourcing and progress	Monthly reporting	HR
Exit Interview Documentation	Departure feedback and insights	Per departure	HR
Diversity and Inclusion Metrics	Team composition and progress	Quarterly reporting	HR
Employee Engagement Surveys	Satisfaction and cultural assessment	Semi-annual execution	HR
Compensation Benchmarking	Market comparison data	Annual update	HR/CFO

STANDARD 16: RESPONSIBLE INVESTMENT STEWARDSHIP

Firms should integrate responsible investment practices. This includes consideration of ESG factors appropriate to investment strategy and investor expectations; responsible investment policies and procedures where applicable to strategy; and stakeholder engagement and stewardship activities as appropriate. Firms should provide transparency in ESG practices and outcomes in investor communications and conduct regular assessment and improvement of ESG integration processes.

Digital assets present unique Environmental, Social, and Governance (ESG) challenges that require tailored frameworks rather than traditional corporate models. For instance, the energy consumption associated with Proof-of-Work (PoW) mining raises significant environmental concerns, whereas decentralized protocols can promote social financial inclusion by expanding economic participation to unbanked populations. Governance in this space deviates from corporate boards to on-chain voting and validator centralization risks. Traditional ESG frameworks are often unsuitable for this asset class because digital asset impact is determined by consensus mechanisms, censorship resistance, and permissionless access rather than standard labor practices or board structures.

Standard 16 emphasizes that firms should adopt responsible investment practices aligned with their specific strategies and investor expectations. This involves creating a dedicated ESG framework that defines the firm's values and identifies the factors most relevant to digital assets. These considerations must be integrated into every stage of the investment lifecycle, from initial protocol screening to ongoing portfolio monitoring. Rather than relying on generic metrics, firms should develop and report on digital-native ESG impacts, engaging directly with protocol developers on sustainability and governance issues while maintaining absolute transparency to avoid "greenwashing."

Effective ESG integration requires customizing strategies to reflect the unique features of the blockchain ecosystem. Analysis should be a value-adding component of the investment process rather than a mere compliance checkbox. Firms must measure actual outcomes—such as carbon offsets or governance participation rates—and communicate these strengths and limitations honestly to investors. As institutional allocators increasingly demand measurable results over simple policy statements, genuine ESG integration builds the long-term credibility and trust necessary for the evolving digital asset space.

16.1 ESG FRAMEWORK AND PHILOSOPHY

A formal ESG framework provides a structured, consistent approach to integrating environmental, social, and governance considerations into the investment lifecycle. Rather than adopting generic traditional asset frameworks, this approach must be specifically tailored to the unique technical and structural characteristics of digital assets.

16.1.1 ESG PHILOSOPHY

The ESG philosophy should be a clear, concise statement outlining the firm's approach to responsible investing. This statement serves as the foundation for all subsequent policy and investment decisions.

- *Core ESG Beliefs:* Define the firm's conviction regarding the impact of ESG on investment outcomes. This includes whether ESG is viewed primarily as a risk management function, a value creation opportunity, or a mandate fulfillment. The philosophy should specify the integration approach, such as using exclusionary screening or identifying ESG factors as a source of alpha.
- *Material ESG Issues:* Identify the specific factors most relevant to the firm's strategy. Digital asset-specific considerations include:
    - Environmental: Energy consumption, consensus mechanism efficiency (e.g., PoW vs. PoS), and the use of renewable energy in mining.
    - Social: Financial inclusion, protocol accessibility, censorship resistance, and the social impact of permissionless infrastructure.
    - Governance: Protocol decentralization, on-chain voting mechanics, validator/miner concentration, and the quality/security of the underlying code.
- *Integration Approach:* Detail how ESG factors influence different stages of the investment process, including initial screening, valuation, position sizing, and ongoing monitoring. The philosophy should outline how conflicts between ESG factors and financial considerations are resolved.
- *Stakeholder Engagement:* Outline the approach to engaging with protocol developers, validators, and other ecosystem participants. This includes the firm's philosophy on participating in on-chain governance and advocating for improved sustainability standards.

16.1.2 ESG POLICY

The formal ESG Policy must be board-approved and reviewed at least annually to ensure it remains current with market and regulatory developments.

- *ESG Framework: Define* the comprehensive framework for integration, including the specific factors considered and the methodology for weighting them. This section should also outline the data sources (e.g., on-chain forensics, ESG ratings providers) and the research processes used.
- *Roles and Responsibilities:* Establish a clear oversight structure, such as an ESG committee. Define the responsibilities of the investment team regarding ESG integration and identify the owners of ESG research, data management, and external reporting.
- *Engagement Approach:* Provide detailed procedures for engaging with portfolio protocols, including guidelines for on-chain governance participation and proxy voting where applicable. Escalation procedures should be defined for cases where ESG concerns are not adequately addressed by a protocol.
- *Measurement and Reporting:* List the specific ESG metrics that will be tracked and reported (e.g., carbon intensity per transaction, decentralization scores). Align reporting with recognized global frameworks.

> ESG frameworks developed for traditional assets may not translate directly to digital assets. Standard metrics—board composition, carbon emissions, labor practices—apply awkwardly to protocols and tokens. Meaningful ESG integration in digital assets requires identifying factors relevant to the asset class: consensus mechanism energy consumption, protocol decentralization, governance concentration, and financial inclusion impact. Best practice is developing ESG criteria specific to digital assets rather than retrofitting traditional frameworks. This should include both risk factors (governance concentration, energy intensity) and opportunity factors (financial inclusion, transparency). The framework should be integrated into investment analysis, not applied as a separate overlay.

16.2 ESG INTEGRATION

ESG integration is the process of incorporating environmental, social, and governance factors into every stage of the investment lifecycle. It goes beyond simple screening; it involves using ESG data to uncover latent risks and identify opportunities that can impact long-term financial performance. For digital asset managers, effective integration means that ESG considerations directly influence asset selection, valuation, and portfolio management.

16.2.1 ESG RESEARCH AND DATA

Firms must establish robust processes for collecting and analyzing specialized digital asset data to overcome the limitations of traditional reporting.

- *Third-Party ESG Data Providers:* Utilize specialized providers that offer digital-native metrics, such as real-time energy consumption estimates by protocol, carbon footprint calculations, and decentralized governance scores.
- *Proprietary ESG Research:* Develop internal insights by analyzing protocol-level factors. This includes evaluating the quality of security audits, developer community health, and the degree of validator or miner centralization.
- *On-Chain Data Analysis:* Leverage the transparency of the blockchain to monitor objective metrics:
    - Governance Dynamics: Tracking participation rates, voting patterns, and treasury management.
    - Technical Health: Monitoring code commits and developer activity on platforms like GitHub.
    - Network Distribution: Assessing validator concentration to identify centralization risks.
- *Primary Research:* Engage directly with protocol teams, attend developer conferences, and participate in industry working groups. Reviewing academic research and technical white papers is essential for understanding the long-term sustainability of emerging technologies.

16.2.2 ESG IN THE INVESTMENT PROCESS

ESG factors should be "hardwired" into the investment workflow to ensure they are consistently applied to every decision.

- *Initial Screening:* Define the investable universe using both Negative Screening (excluding protocols that fail to meet minimum environmental or governance

standards) and Positive Screening (prioritizing "best-in-class" assets with high ESG scores).

- *Due Diligence:* Conduct deep-dive assessments into governance quality, environmental impact (PoW vs. PoS), and code security. As of 2026, many managers also evaluate regulatory alignment as a key ESG due diligence component.
- *Valuation and Position Sizing:* Incorporate an "ESG risk premium" or discount into valuation models. Higher-risk ESG assets may face stricter concentration limits or reduced position sizes to protect the overall portfolio from volatility.
- *Ongoing Monitoring:* Continuously track ESG performance. Monitoring should include alerts for governance changes, security incidents, or shifts in the carbon intensity of a protocol's network.
- *Exit Decisions:* Material ESG deterioration—such as a governance failure, a significant security breach, or a persistent increase in environmental impact—should trigger a formal review and potential exit of the position.

ESG integration applied only as post-hoc screening provides limited value—positions can only be rejected, not improved through the integration. Effective integration incorporates ESG factors into initial analysis, potentially influencing security selection, position sizing, and engagement priorities.Best practice is embedding ESG analysis in the investment process from initial screening through ongoing monitoring. Analysts should document how ESG factors influenced investment decisions—not just whether positions passed screening, but how ESG analysis shaped the investment thesis or position parameters. This integration demonstrates that ESG is substantively considered, not just procedurally applied.

16.3 ESG REPORTING & TRANSPARENCY

ESG reporting gives investors clear and transparent details about a company's ESG efforts and results. This helps build trust with investors. More and more, organizations are required to provide ESG reports before they can receive investments. Good ESG reporting should be easy to understand, include important information, and avoid unnecessary details. It should focus on key facts that matter most to investors, making it simple and straightforward to evaluate a company's ESG performance.

16.3.1 ESG REPORTING FRAMEWORK

As of 2026, the global ESG reporting landscape has consolidated around the International Sustainability Standards Board (ISSB), which has integrated legacy frameworks into a single global baseline. Investment managers should align their reporting with these unified standards to ensure institutional-grade consistency.

- *IFRS S1 & S2 (The New Global Baseline):* The ISSB's standards, IFRS S1 (General Requirements) and IFRS S2 (Climate-related Disclosures), have now superseded the individual TCFD and SASB frameworks.
    - SASB Integration: The industry-specific metrics originally developed by SASB are now fully embedded within IFRS S1, providing standardized, sector-specific disclosures.
    - TCFD Integration: The TCFD disbanded in late 2023, and its four pillars (Governance, Strategy, Risk Management, and Metrics/Targets) are now the core foundation of IFRS S2.
- *PRI (Principles for Responsible Investment):* A voluntary set of six principles for ESG integration. Signatories are required to provide annual reports, which are then tiered and benchmarked against peers.
- *Digital Asset-Specific Frameworks:* Emerging industry standards from trade associations (such as ADAM or GDF) provide specialized metrics for blockchain-specific risks, such as protocol-level decentralization scores and real-time energy intensity per transaction.

16.3.2 KEY COMPONENTS OF AN ESG REPORT

A high-quality institutional ESG report should go beyond policy statements to provide measurable, data-driven insights.

- *ESG Philosophy and Framework Overview:* A concise statement of the firm's core ESG beliefs, a description of the factor weighting methodology, and an overview of the governance structure responsible for ESG oversight.
- *Performance Data and Metrics:*
    - Climate Impact: Quantitative estimates of the portfolio's carbon footprint, specifically focusing on the energy intensity of different consensus mechanisms (e.g., PoW vs. PoS).
    - Governance Quality: Quantitative scores for protocol decentralization and transparency.
- *Case Studies:* Real-world examples where ESG analysis directly influenced an investment decision, such as avoiding a protocol due to governance centralization or increasing exposure to a "best-in-class" energy-efficient network.
- *Engagement and Governance:* A summary of on-chain governance participation, including proxy voting records and active engagement with protocol developers to improve sustainability or security.
- *Forward-Looking Initiatives:* A roadmap for planned improvements, such as committing to net-zero targets for firm operations or investing in new research focused on the social impact of financial inclusion through DeFi.

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional allocators evaluate ESG integration through implementation evidence rather than policy statements. Allocators distinguish between firms with systematic ESG integration demonstrating measurable impact on portfolio construction and those maintaining aspirational policies without operational implementation. Inability to provide specific examples of ESG-driven investment decisions or produce substantive proprietary research reveals ESG programs exist for marketing rather than genuine integration.

ESG Framework and Integration

- Walk through your ESG framework—what specific ESG factors do you consider material to digital asset investment outcomes?
- How do you integrate ESG into your investment process and at what decision points do ESG considerations influence analysis?

- Provide specific examples of investments where ESG analysis materially influenced the decision.
- What ESG data sources and research do you utilize?
- How do you assess digital asset-specific ESG factors—energy consumption, protocol governance, validator centralization, code audit quality?

ESG Measurement and Reporting

- What ESG reporting framework do you use? Provide your most recent ESG report showing actual portfolio ESG characteristics and performance.
- How do you measure ESG impact—what metrics track outcomes rather than just inputs?
- Walk through how ESG metrics evolved over the past year. Static metrics suggest inadequate monitoring.

Portfolio Engagement

- How do you engage with portfolio companies or protocols on ESG issues? For liquid strategies, describe governance participation. For venture strategies, describe board engagement.
- Provide examples of recent ESG engagement including the issue, your position, and outcome.
- What is your proxy voting record on ESG-related proposals? For protocols, how do you participate in on-chain governance?

Documentary Evidence Requirements

- Complete ESG policy with investment process integration points
- Most recent ESG report showing portfolio metrics and evolution
- Examples of proprietary ESG research beyond third-party ratings
- Engagement log with portfolio interactions and outcomes
- Proxy voting or governance participation records with rationale
- Portfolio construction documentation showing ESG-influenced decisions

COMMON PITFALLS & REMEDIATION

- *ESG claims exceed verifiable reality*. Marketing emphasizes sustainability commitment but actual practices don't support the claims. "ESG-integrated" label applied without documented methodology, measurable criteria, or demonstrable impact on investment decisions. Remediation: Ensure every ESG claim is supportable with evidence. Report specific metrics with methodology disclosed. Acknowledge program limitations honestly—credibility comes from accuracy, not aspiration. Focus communication on what you actually do, not what you aspire to do.
- *ESG treated as compliance overlay, not investment input*. ESG exists as separate workstream producing reports but not influencing investment decisions. Analysis performed after positions taken rather than informing selection or sizing. Integration is nominal. Remediation: Embed ESG analysis in investment process from initial screening through ongoing monitoring. Document specifically how ESG factors influenced decisions—not just that analysis was performed, but what changed as a result. If ESG analysis never affects a decision, it's not integrated.
- *ESG framework static despite evolving landscape*. Criteria established at program launch but never updated as understanding deepens, data improves, or regulatory expectations change. Framework becomes increasingly disconnected from current best practices and stakeholder expectations. Remediation: Review ESG framework at least annually. Update criteria to reflect regulatory developments (particularly emerging disclosure requirements), improved data availability, and lessons learned from portfolio experience. Document changes and rationale for evolution.
- *ESG reporting lacks measurable outcomes*. Reports describe policies and intentions but provide no metrics, no trend data, and no way to assess whether program is effective or improving. Narrative without numbers can't demonstrate progress. Remediation: Define specific, measurable ESG metrics appropriate to strategy. Track consistently over time and report trends—improvements and regressions. Use concrete examples showing how ESG integration affected specific decisions or outcomes. Year-over-year comparison enables accountability.
- *No governance oversight of ESG claims*. ESG statements made in marketing and investor communications without independent validation. No committee or function responsible for verifying claims are accurate and methodology is sound. Remediation: Assign ESG oversight to designated committee (ESG Committee, Risk Committee, or board). Review ESG claims before publication for accuracy

and supportability. Maintain documentation of methodology and evidence supporting reported metrics. Consider external assurance for material claims as program matures.

16.5 KEY CONTROLS & DOCUMENTATION

Document	Purpose	Update Frequency	Owner
ESG Policy	Comprehensive framework and commitments	Annual	CIO
Integration Procedures	ESG incorporation into investment process	Semi-annual	Investment Team
Scoring Methodology	ESG scoring factors, weights, calculations	Annual	CIO
Voting Policy	Governance participation guidelines	Annual	CIO
Engagement Records	Protocol engagement documentation	Ongoing	Investment Team
Impact Metrics Tracking	ESG performance monitoring	Quarterly	Analyst
Annual ESG Report	Comprehensive public disclosure	Annual	CIO
Vendor ESG Assessment	Service provider evaluation	Annual	Operations
Corporate Sustainability	Internal organizational initiatives	Ongoing	Operations/HR

STANDARD 17: SERVICE PROVIDERS & PROFESSIONAL RELATIONSHIPS

Firms must establish and maintain professional relationships with qualified service providers across all critical operational functions. This includes fund administrators, custodians, prime brokers, independent auditors with digital asset expertise, legal counsel, compliance consultants, and technology vendors. Firms must conduct comprehensive due diligence before engagement, negotiate clear service level agreements, implement ongoing performance monitoring, and maintain contingency plans for provider transitions. Annual independent audits by qualified firms with digital asset experience verify financial statements and provide institutional credibility.

External providers in digital asset management can pose significant operational risks and create critical dependencies. Failures by these providers can lead to systemic disruptions, and in many cases, a provider's lack of specialized expertise may hide latent risks within the infrastructure. When incentives are not aligned, the quality of service—particularly in areas like security and reporting—can suffer. The market for high-quality, institutional-grade digital asset services is still maturing, which often leaves firms with few reliable options. Historically, reconciling third-party custody, managing inconsistent audit quality, and navigating unreliable APIs have reduced operational efficiency. Notable failures such as the issues at Celsius, the total collapse of FTX, and various high-profile security breaches serve as stark reminders of the vulnerabilities inherent in poorly managed external relationships.

Standard 17 emphasizes that firms must professionally manage all external relationships to mitigate these risks. This involves conducting thorough, ongoing due diligence that goes beyond initial onboarding, establishing clear and enforceable service-level agreements (SLAs), and regularly reviewing provider performance against key risk indicators. Ensuring robust legal and compliance support is essential for defining liability and asset recovery protocols. Furthermore, maintaining adequate insurance coverage—either through the provider or the firm itself—is a critical safety net. While outsourcing allows a firm to leverage external expertise, the firm remains ultimately responsible to its clients for any failures that occur within its service chain.

Managing external providers effectively requires treating selection as a core risk decision rather than a procurement task. It is essential to prioritize institutional-grade quality over cost, as the "cheapest" providers often lack the redundant security and capital reserves

necessary to survive a crisis. Continuous monitoring of provider performance, coupled with the development of robust contingency plans (such as "exit strategies" to move assets to a backup custodian), helps reduce operational downtime. Making cost-based decisions without considering provider quality is a primary driver of operational failure; therefore, building long-term, transparent relationships with reliable providers is essential for a stable and resilient digital asset management firm.

17.1 SERVICE PROVIDER ECOSYSTEM MANAGEMENT

Digital asset managers depend on complex ecosystems of specialized service providers whose operational failures can create immediate, and often irreversible, disruption. Unlike traditional finance, where providers like fund administrators or custodians are largely commoditized with standardized capabilities, the digital asset service provider landscape in 2026 demonstrates wide quality variation. This necessitates a "trust-but-verify" approach, where selection and monitoring are treated as high-stakes risk management decisions.

17.1.1 SERVICE PROVIDER UNIVERSE

A firm's operational infrastructure is only as resilient as its weakest link. For institutional managers, the ecosystem is categorized into seven critical pillars:

TABLE 1: SERVICE PROVIDER MATRIX

Category	Primary Function	Institutional Selection Criteria
Fund Administrator	NAV calculation, bookkeeping, and investor reporting.	Must handle on-chain reconciliation and complex DeFi transaction types; expertise in fair-value pricing for illiquid tokens.
Custodians	Safeguarding private keys and digital property.	Focus on MPC (Multi-Party Computation) architectures, bankruptcy-remote structures, and high-limit insurance coverage.
Prime Brokers	Financing, margin, and cross-venue trade execution.	Assessment of capital reserves, collateral mobility, and reliability of settlement APIs during high-volatility periods.
Legal Counsel	Regulatory guidance and contract negotiation.	Deep knowledge of the GENIUS Act (2026) and evolving global token classifications (e.g., MiCA, MAS).

Category	Primary Function	Institutional Selection Criteria
Compliance Consultants	Program design and exam preparation.	Expertise in blockchain transaction monitoring and preparing firms for digital-native regulatory examinations.
Technology Vendors	PMS, OMS, and risk management platforms.	Real-time data integration with blockchain nodes and seamless API connectivity to multiple custodial and execution venues.
Auditors	Independent financial statement verification.	Specialized procedures for "Proof of Reserve" verification and testing of internal cryptographic controls.

Critical Assessment Pillars for 2026

- *Fund Administration & Accounting:* In 2026, administrators are expected to provide "shadow NAV" capabilities that sync with real-time on-chain data. They must bridge the gap between traditional fiat ledgering and the 24/7 nature of digital markets, often using API-driven automated reconciliation to handle thousands of micro-transactions.
- *Custodial Rigor:* Following the regulatory refinements of 2025, institutional custodians must demonstrate Qualified Custodian status under updated federal rules. Evaluation should prioritize providers with SOC 1 Type II and SOC 2 Type II certifications that specifically cover private key generation and signing ceremonies.
- *Technological Interoperability:* A vendor's value in 2026 is measured by its interoperability. Siloed systems are a risk; the preference is for "composite architectures" where a PMS (Portfolio Management System) can communicate directly with a hardware security module (HSM) or MPC wallet to verify assets in real-time.

Service provider selection based primarily on cost or existing relationships, without systematic evaluation of capability and stability, may result in providers unable to meet institutional expectations. Service provider quality reflects on the firm—failures or deficiencies become the firm's problems regardless of where fault lies. Best practice is conducting documented competitive evaluation for material service provider relationships, assessing: relevant experience and expertise, operational capability and capacity, financial stability, reference feedback, and terms including service levels and termination provisions. The selection rationale should be documented, supporting the conclusion that the chosen provider best serves investor interests.

17.1.2 SERVICE PROVIDER DUE DILIGENCE AND MONITORING

The process for selecting and overseeing service providers must be formal, rigorous, and documented. Because the digital asset landscape is technically complex and subject to rapid regulatory shifts, firms must implement a "lifecycle" approach to third-party risk. This ensures that selection is fair, performance is consistent, and the firm remains resilient even if a provider fails.

Due Diligence (Pre-Selection)

Before onboarding, firms must conduct a thorough "deep dive" into a provider's operational and financial health. In 2026, due diligence should include:

- *Business & Financials:* Reviewing audited financial statements and insurance policies (specifically E&O, cyber, and crime/theft).
- *Technical Security:* Assessing private key management (MPC vs. Multi-sig), hardware security modules (HSMs), and API reliability.
- *Regulatory Standing:* Verifying current licenses and reviewing past regulatory examination findings or enforcement actions.
- *Operational Resilience:* Testing the provider's Business Continuity Plan (BCP) and Disaster Recovery (DR) capabilities specifically for digital asset recovery.

Contract Negotiation (Service Level Agreements)

A comprehensive Service Level Agreement (SLA) is the primary legal tool for defining accountability. Essential components include:

- *Performance Standards:* Defining clear "uptime" requirements, withdrawal turnaround times, and reporting deadlines.
- *Liability & Indemnification:* Specifying who bears the risk of loss in the event of a hack, error, or provider insolvency.
- *Data & Portability:* Establishing clear ownership of data and ensuring "exit assistance" to facilitate moving assets or records if the relationship is terminated.
- *Compliance Requirements*: Mandating the provider's adherence to global standards, such as the Travel Rule and SOC 2 Type II reporting.

Ongoing Monitoring

Initial due diligence is insufficient; firms must continuously monitor providers to detect "risk drift."

- *Performance Reviews:* Conducting quarterly business reviews (QBRs) and annual deep-dive assessments.
- *Real-time Incident Tracking:* Monitoring for errors, system outages, or breaches.
- *Stability Re-assessment:* Regularly verifying the provider's capital adequacy and regulatory status to ensure they remain a viable institutional partner.

Contingency Planning

Firms must operate under the assumption that a provider could fail. To mitigate this "concentration risk," the following measures are required:

- *Secondary Providers:* Identifying "warm" backup providers for critical services, such as a second qualified custodian or an alternative administrator.
- *Migration Playbooks:* Developing step-by-step procedures for transferring assets and migrating data to an alternative provider without halting operations.
- *Data Redundancy:* Maintaining independent backups of all books and records provided by the administrator to ensure the firm can reconstruct its history if the provider goes offline.

Managing service providers is not a one-time task; it requires ongoing effort. Regular meetings and performance reviews are essential to ensure quality and address issues promptly. When evaluating management, request important documents such as due diligence reports, service level agreements, review notes, assessment results, and examples of past problems and how they were resolved. During due diligence, ask questions like: "*Can you walk me through how you would handle a major failure that requires replacing a service provider? What are your contingency plans and how quickly can you transition?*" If they cannot clearly explain these points, it may indicate poor risk management. Proper ongoing management helps protect investments and ensures service providers meet expectations consistently.

17.2 AUDIT MANAGEMENT AND COORDINATION

The annual audit constitutes a critical component of the financial reporting process. A well-defined process for managing and coordinating the audit ensures timely completion and appropriate quality. Audit quality in digital assets varies dramatically based on auditor expertise; generalist auditors often apply traditional procedures that are inadequately adapted to digital asset operations, potentially missing material risks such as cryptographic control failures or improper valuation of illiquid tokens.

17.2.1 AUDITOR SELECTION

Selecting an auditor with specific experience in the digital asset industry is paramount. Firms should evaluate candidates based on the following criteria:

- *Digital Asset Expertise:* Assess the number of years the firm has conducted digital asset audits and the percentage of their practice dedicated to the sector. The audit team must demonstrate a deep understanding of custody verification, on-chain transaction flows, and the complexities of DeFi protocols.
- *Technical Capabilities:* Evaluate the firm's proprietary tools and methodologies for blockchain verification. This includes their approach to verifying multi-signature arrangements, reconstructing transactions from block explorers, and their methodology for valuing illiquid or low-liquidity tokens.
- *Independence and Reputation:* Consider the firm's standing in the digital asset markets and review any regulatory scrutiny or peer review findings. Verification of independence and a thorough conflict-of-interest assessment are mandatory.

- *Service Quality:* Look for engagement team consistency year-over-year and a reasonable fee structure. A high-quality auditor provides value-added observations and recommendations that improve the firm's overall operational posture.

17.2.2 AUDIT PLANNING AND COORDINATION

Effective coordination with the auditor throughout the lifecycle of the engagement reduces friction and accelerates the delivery of the final report.

- *Pre-audit Planning:* A formal planning meeting should occur 90 days before year-end. This meeting covers the audit scope, materiality determination, and significant accounting judgments such as revenue recognition and valuation. Reviewing prior-year findings ensures that previous weaknesses have been remediated.
- *Audit Package Preparation:* Firms should maintain "audit-ready" documentation continuously rather than scrambling at year-end. A standard audit package includes:
    - Draft financial statements and reconciliations.
    - Third-party custody confirmations.
    - Transaction listings and supporting schedules for all on-chain activity.
- *Audit Execution:* Establish a regular communication cadence with the audit team to address queries promptly. Ensure auditors have direct access to necessary personnel, systems, and service providers (e.g., fund administrators). Interim meetings should be used to review progress and preliminary findings before the final review.
- *Management Letter Response:* Upon receiving the management letter, the firm must conduct a thorough review to understand the root causes of any identified weaknesses. Response plans should include specific remediation actions, assigned responsible parties, and firm completion dates, which are then verified during the subsequent audit cycle.

Audit quality in digital assets varies widely depending on auditor expertise, as generalists often overlook key risks like custody controls, valuation, and transaction integrity. Specialized auditors understand these nuances and follow procedures tailored to the blockchain. When evaluating a manager, allocators should request firm information, recent financials, management letters, and specific audit procedures. During due diligence, it is critical to ask: "*How does your auditor verify custody and assets, and what specific procedures do they perform that go beyond standard balance confirmations?*" Generic answers regarding standard confirmations that lack mentions of blockchain verification or multi-signature checks indicate inadequate digital asset expertise and a potential failure to capture material operational risks.

17.3 LEGAL AND COMPLIANCE ADVISORY

Investment managers require sophisticated legal and compliance guidance to navigate a maturing but complex regulatory landscape. In the current environment, the shift from pure enforcement to clearer legislative frameworks has increased the importance of building deep partnerships with specialized law firms and compliance experts. These advisors are essential for translating technical blockchain realities into defensible institutional practices.

17.3.1 LEGAL COUNSEL

Legal advisors must be trusted experts who bridge the gap between traditional securities law and digital asset innovation. They provide the structural and strategic foundation for the firm's operations.

- *Fund Formation and Structuring:* Guidance on domestic and offshore vehicles, including the selection of tax-optimized jurisdictions (e.g., Cayman, BVI, or Luxembourg). They ensure offering documents meet investor suitability requirements and manage all necessary regulatory filings.
- *Regulatory Compliance:* Interpreting the convergence of major frameworks, such as the EU's fully operational MiCA standards and the U.S. CLARITY and GENIUS Acts. Advisors provide the "regulatory defense" necessary for examinations and ensure firms meet harmonized global standards for licensing and disclosure.
- *Specialized Technical Guidance:* Performing rigorous analysis for token classifications, staking, and yield generation to ensure compliance with evolving

securities laws. This includes legal audits of DeFi protocol interactions and cross-border jurisdictional requirements.

- *Contract Negotiation:* Negotiating critical service provider agreements, specifically for Prime Brokerage and Custody. They ensure that contracts address 2026-specific risks like "collateral mobility" and sub-custodial liability.
- *Dispute Resolution:* Providing defense for regulatory enforcement actions and representing the firm in investor arbitrations or intellectual property matters related to proprietary code or branding.

17.3.2 COMPLIANCE CONSULTANT

A compliance consultant provides the "engine" for the Chief Compliance Officer (CCO), assisting with regulatory adherence and risk management in an environment where "compliance-by-design" is the new institutional standard.

- *Program Development:* Implementing a comprehensive compliance program that incorporates the latest Financial Stability Board (FSB) and IOSCO recommendations for market integrity and investor protection.
- *Annual Reviews and Testing:* Conducting mandatory annual reviews and "mock exams" to identify operational weaknesses before official regulatory audits occur.
- *Global Monitoring & Travel Rule:* Managing the technical complexities of the Crypto Travel Rule, ensuring the secure exchange of originator and beneficiary information across all jurisdictions, regardless of local regulatory maturity.
- *On-Chain Surveillance*: Utilizing advanced blockchain forensic tools for AML transaction monitoring, sanctions screening, and personal trading surveillance to detect market abuse in real-time.
- *Training and Change Management:* Developing training programs to keep employees updated on the rapid evolution of digital asset laws, ensuring a culture of compliance that protects the firm’s reputation.

Legal advice quality depends on advisor expertise relevant to the specific matter. General corporate counsel may lack familiarity with digital asset-specific regulatory nuances across SEC, CFTC, FinCEN, and state regimes. Complex regulatory environment makes specialized expertise particularly valuable. Best practice is engaging legal advisors with demonstrated digital asset experience for crypto-specific matters, while maintaining appropriate general corporate counsel for broader needs. For material regulatory questions, advisor experience with similar issues for similar clients provides confidence that advice reflects current practice and regulatory expectations.

17.4 INSURANCE AND RISK TRANSFER

Directors and Officers (D&O) insurance serves as a critical mechanism for transferring liability risks from the firm and its leadership to insurance carriers. Digital asset managers operate under heightened litigation and regulatory risks driven by operational complexity and the global implementation of new regulatory frameworks. Market volatility frequently triggers investor disputes, and regulatory scrutiny has become more forensic, making robust insurance coverage a prerequisite for institutional credibility.

17.4.1 DIRECTORS AND OFFICERS INSURANCE COVERAGE

D&O insurance is designed to protect company leaders and the entity itself from the financial impact of legal actions, government investigations, or investor disagreements. To provide institutional-grade protection, a policy must include three distinct components:

- **Coverage Components:**
    - *Side A:* Safeguards the personal assets of individual directors and officers when the firm is legally or financially unable to indemnify them (e.g., in cases of insolvency).
    - *Side B:* Reimburses the firm when it has already indemnified its leaders for their legal costs or settlements.
    - *Side C (Entity Coverage):* Directly protects the firm's balance sheet when it is named as a defendant in a securities-related claim.
- **Coverage Limits and Benchmarking:** Institutional allocators typically set minimum coverage requirements as a condition for mandate awards. While specific limits depend on risk profile, current industry benchmarks include:

- *AUM < $100M:* $1M – $2M in coverage.
- *AUM $100M – $250M:* $2M – $5M in coverage.
- *AUM $250M – $500M:* $5M – $10M in coverage.
- *AUM > $500M:* Upwards of $10M+, often requiring "layered" excess coverage.

- **Digital Asset-Specific Provisions:** Standard D&O policies often contain broad "crypto exclusions" that must be formally removed or modified. Managers must ensure their policy explicitly covers digital asset activities, regulatory investigations, and employment practices. Given the rise of AI-driven exploits in 2026, firms should verify that their D&O policy either includes or is supplemented by a standalone Cyber Liability policy to cover data breaches and "portfolio extortion" risks.

17.4.2 INSURANCE MANAGEMENT

Effective insurance management is an ongoing fiduciary responsibility that requires regular calibration as the firm evolves.

- *Carrier Selection and Underwriting:* Choose carriers with a minimum financial rating of A- and proven experience in digital asset underwriting. Firms should be prepared to share their Business Continuity Plans (BCP) and threat monitoring data during the underwriting process.
- *Policy Maintenance and Renewals:* Conduct an annual review of coverage limits relative to current AUM and risk exposure. Application disclosures must be updated to reflect material changes—such as new tokenized asset offerings or shifts in custodial partners—to prevent insurers from denying claims based on "non-disclosure" of material facts.
- *Claims and Incident Management:* Establish a protocol for immediate carrier notification upon the occurrence of a "trigger event," such as a formal regulatory inquiry or a significant investor dispute. Working closely with legal counsel during the notification phase ensures that documentation is preserved and the claim is handled according to policy requirements.

D&O Insurance in digital assets is costly due to increased regulatory and operational risks. Firms cut costs with insufficient coverage or exclusions, risking worthless coverage during claims. Cost-conscious strategies lead to catastrophic exposure when risks exceed policy limits or fall under exclusions. Assessors request current D&O policy details, carrier info, exclusions, claims history, and proof of adequacy during due diligence. A key question is to explain coverage limits, exclusions, and how adequacy is determined. Failing to clarify coverage or defensively addressing costs indicates poor risk management, risking personal liability for directors officers.

17.5 REGULATORY & INDUSTRY ENGAGEMENT

A firm's reputation is no longer built solely on performance, but on its active presence within the regulatory and professional ecosystem. Strong industry engagement signals to institutional investors that a manager is not just a participant, but a leader committed to the long-term integrity of the market. Proactive relationships with regulators act as a "compliance buffer," often leading to more efficient examinations and a more predictable operational environment.

17.5.1 REGULATORY RELATIONSHIP MANAGEMENT

A professional, transparent relationship with regulators is a strategic asset. By treating regulators as stakeholders rather than adversaries, firms can navigate "regulatory recalibration"—characterized by more tailored, localized rules—with greater agility.

- *Proactive Communication:* Do not wait for an examination to engage. Maintain an open dialogue regarding novel investment strategies, shifts in custody architecture, or the adoption of agentic AI in trading. Seeking informal "staff guidance" on ambiguous mandates demonstrates a culture of "compliance-by-design."
- *Examination Cooperation:* Treat regulatory reviews as a partnership in risk management. Provide examiners with "read-only" access to real-time compliance dashboards and on-chain monitoring tools. Construction of comprehensive remediation plans for any identified deficiencies shows a commitment to institutional excellence.
- *Enforcement & Response:* In the event of an inquiry or action, engage specialized counsel immediately. Today regulators prioritize firms that self-report errors and

implement remediation that exceeds minimum requirements, often viewing such honesty as a sign of high-quality internal governance.

17.5.2 INDUSTRY ENGAGEMENT

Active participation in trade associations and working groups is essential for staying ahead of global standards and influencing the "rules of the road" for the next decade of digital finance.

- *Standards Development:* Contribute to industry-wide initiatives, such as establishing unified "Proof of Reserve" protocols or standardized ESG metrics for proof-of-stake validators.
- *Thought Leadership:* Publish research on market structure, institutional-grade DeFi, or the impact of Real-World Asset (RWA) tokenization. Speaking at institutional market conferences builds brand equity and attracts top-tier talent.
- *Regulatory Advocacy:* Support reasonable, innovation-friendly frameworks by participating in public comment periods. Advocacy that prioritizes market integrity and investor protection aligns the firm's interests with those of its most sophisticated institutional clients.

ALLOCATOR DUE DILIGENCE CONSIDERATIONS

Institutional investors assess external partners based on the quality of their services, the thoroughness of their audits, and their professional reputation, rather than just focusing on cost savings.

Service Provider Selection and Monitoring

- Who are your key service providers and what is your process for selecting and monitoring them?
- Walk through your service provider selection process—what due diligence was conducted, what alternatives were evaluated, and what criteria drove final selection?
- How do you monitor service provider performance on an ongoing basis?
- Describe a recent service provider issue and how it was resolved.
- What contingency arrangements exist if a critical service provider fails?

Audit Quality and Management

- Who is your auditor and what specific digital asset experience do they possess?
- Can I see your most recent audited financial statements?
- Walk through your audit coordination process—how do you prepare and what challenges arise?
- Has your auditor issued management letters identifying control weaknesses? Provide letters and remediation documentation.
- How many years has the current auditor served?

Legal and Compliance Expertise

- Who provides legal and compliance advice and what specific digital asset expertise do they possess?
- Provide examples of significant legal or compliance guidance received in past year.
- How do you manage legal costs while maintaining access to specialized expertise?

Insurance and Professional Standing

- What D&O insurance coverage do you maintain? Provide policy declarations.
- How does your coverage compare to your assets under management?
- What industry associations are you members of and what leadership roles do you hold?
- What regulatory examinations have you undergone and what were the outcomes?

Documentary Evidence Requirements

- Complete list of material service providers with services, duration, and contacts
- Service provider due diligence files and selection documentation
- Service level agreements with performance standards
- Service provider performance monitoring documentation
- Most recent audited financial statements
- Audit management letters with remediation documentation
- Legal and compliance advisor engagement letters
- D&O insurance policy declarations

COMMON PITFALLS & REMEDIATION

- *Service providers selected without rigorous diligence*. Administrator, auditor, or custodian chosen based on referral, existing relationship, or cost without systematic evaluation of capability, expertise, and stability. Provider limitations discovered only when problems arise. Remediation: Implement formal due diligence for all material service providers covering: operational capabilities, digital asset-specific expertise, financial condition, regulatory standing, and client references. Document evaluation criteria and selection rationale. Provider quality reflects on your firm—choose accordingly.
- *Provider relationships unmonitored after onboarding*. Initial due diligence performed but ongoing oversight neglected. Service quality degrades, key personnel depart, or control environment weakens without detection. Firm assumes continued adequacy without verification. Remediation: Establish systematic provider monitoring: quarterly business reviews assessing service quality and relationship health, monthly performance tracking against SLAs, and annual due diligence refresh. Address issues promptly—tolerance for persistent underperformance enables decline.
- *Auditor lacks digital asset expertise*. Firm engages reputable auditor but engagement team has no crypto experience. Traditional audit procedures applied without adaptation for wallet verification, DeFi position valuation, or blockchain transaction testing. Audit provides limited assurance on digital asset-specific risks. Remediation: Select auditors with demonstrated digital asset experience—not just firm capability, but specific engagement team credentials. Request client references from similar funds. Verify team understands custody verification, on-chain transaction testing, and crypto-specific valuation challenges.
- *Audit relationship treated as adversarial*. Auditor viewed as obstacle rather than control validation. Information provided reluctantly, issues minimized or obscured, and recommendations resisted. Adversarial dynamic undermines audit effectiveness and raises questions about what firm is hiding. Remediation: Embrace audit as independent validation that strengthens investor confidence. Disclose issues proactively rather than waiting for discovery. Implement recommendations systematically and track to completion. Constructive audit relationships benefit everyone—including the firm.
- *Legal counsel lacks specialized expertise*. Firm relies on general corporate attorney or securities generalist for digital asset-specific matters. Counsel unfamiliar with CFTC requirements, state money transmitter analysis, custody regulation

nuances, or cross-border considerations. Advice may miss crypto-specific issues. Remediation: Engage counsel with demonstrated digital asset expertise for regulatory and compliance matters. Evaluate through published thought leadership, conference presence, and regulatory defense experience. Specialized expertise matters—digital asset regulation is too complex and evolving for generalists to navigate reliably.

- *D&O and E&O insurance inadequate or absent*. Directors, officers, and firm lack appropriate liability coverage. Policy obtained without reviewing exclusions, coverage limits insufficient for actual exposure, or carrier financial strength questionable. Protection proves illusory when claim arises. Remediation: Obtain D&O and E&O coverage from financially strong carriers with experience insuring investment managers. Review policy exclusions carefully—crypto-specific exclusions may limit coverage significantly. Size limits appropriately for firm scale and risk profile. Review annually as firm evolves.
- *Industry participation superficial or absent*. Firm operates in isolation without engagement in industry associations, standards bodies, or regulatory dialogue. Misses early visibility into regulatory developments, best practice evolution, and peer relationships that provide support during challenges. Remediation: Engage meaningfully in relevant industry initiatives—SBAI, AIMA, or digital asset-specific groups. Participate in committees, contribute to standards development, and share expertise through thought leadership. Industry engagement builds relationships, credibility, and early awareness of emerging issues.

KEY CONTROLS & DOCUMENTATION

Document Type	Purpose	Update Frequency	Ownership
Service Provider Register	List of providers with contracts and SLAs	Quarterly review	COO
Service Provider Due Diligence Files	Selection process documentation	Per engagement	COO
Audit Management File	Year-round audit readiness	Continuous	CFO

Document Type	Purpose	Update Frequency	Ownership
Management Letter Tracking	Audit findings and remediation	Per audit	CFO
Legal Opinion Repository	Database of legal advice	Ongoing	General Counsel
Insurance Policy Register	All policies with coverage details	Annual review	CFO
Industry Engagement Log	Association participation	Ongoing	CE0
Regulatory Correspondence File	Communications with regulators	Ongoing	CCO

APPENDIX: GLOSSARY OF TERMS

- **Accredited Investor**: An investor meeting SEC Regulation D financial thresholds including $1 million net worth (excluding primary residence) or $200,000 annual income ($300,000 joint).
- **Administrator**: Third-party service provider responsible for fund accounting, NAV calculation, investor reporting, and related middle-office functions.
- **Air-Gapped System**: Computer or network physically isolated from unsecured networks including internet connection.
- **Airdrop**: Distribution of cryptocurrency tokens to wallet addresses, typically as a promotional mechanism or reward for protocol participation, which may trigger tax obligations and require operational procedures for receipt and disposition.
- **Anti-Money Laundering (AML)**: Legal controls and procedures designed to prevent, detect, and report money laundering activities.
- **Atomic Swap**: Direct peer-to-peer cryptocurrency exchange executed through smart contracts without intermediary.
- **Audit Committee**: Board committee responsible for overseeing financial reporting, external audit coordination, internal control assessment, and compliance program review.
- **Audit Trail**: Chronological record documenting sequence of activities affecting specific operation, procedure, or event.
- **Automated Market Maker (AMM)**: Decentralized exchange protocol that uses algorithmic pricing based on liquidity pool reserves rather than traditional order books to facilitate token swaps.
- **Basis Risk**: Risk that offsetting positions in a hedging strategy do not move in perfectly opposite directions, resulting in imperfect correlation between the hedge and underlying exposure.
- **Beneficial Ownership**: The natural persons who ultimately own or control a legal entity, typically those owning 25% or more equity interests or exercising significant control, as required under FinCEN Customer Due Diligence rules.
- **Best Execution**: Duty to seek most favorable terms reasonably available under the circumstances for client transactions considering price, speed, likelihood of execution, and total costs.

- **BitLicense**: New York State Department of Financial Services license required for businesses engaged in virtual currency business activities involving New York residents, imposing capital, compliance, cybersecurity, and examination requirements.
- **Blockchain**: Distributed ledger technology recording transactions across multiple nodes in verifiable, permanent way.
- **Blockchain Analytics**: Tools and techniques for analyzing blockchain transaction data to identify patterns, trace fund flows, screen for sanctions exposure, detect suspicious activity, and support AML compliance.
- **Board of Directors**: Governing body responsible for overseeing management, providing strategic direction, and fulfilling fiduciary duties to the organization and its stakeholders.
- **Break Resolution**: Process of identifying, investigating, and correcting discrepancies between internal records and external statements, including reconciliation differences with custodians, administrators, or counterparties.
- **Bridge**: Protocol enabling transfer of tokens or data between different blockchain networks.
- **Business Continuity Plan (BCP)**: Documented procedures for maintaining or recovering business operations following disruption.
- **Centralized Exchange (CEX)**: Cryptocurrency trading platform operated by centralized entity maintaining order books and custody.
- **Chief Compliance Officer (CCO)**: Individual responsible for administering firm's compliance policies, procedures, and regulatory obligations.
- **Chief Operating Officer (COO)**: Executive responsible for firm's day-to-day operational activities and business execution.
- **Chief Risk Officer (CRO)**: Executive responsible for enterprise risk management, including identification, measurement, monitoring, and mitigation of risks across the organization, with independent reporting to the board or CEO.
- **Cold Storage**: Cryptocurrency storage method where private keys remain offline and disconnected from any network.
- **Collateral**: Assets pledged to secure borrowing, derivatives positions, or other obligations.
- **Collateralization Ratio**: The ratio of collateral value to borrowed amount or position exposure, used to determine margin adequacy and liquidation thresholds in lending and derivatives contexts.

- **Commodity Pool Operator (CPO)**: Entity registered with the CFTC that operates pooled investment vehicles trading commodity futures, options, or swaps, subject to disclosure, reporting, and segregation requirements.
- **Commodity Trading Advisor (CTA)**: Entity registered with the CFTC that provides advice on commodity futures, options, or swaps trading, subject to Series 3 examination, NFA membership, and disclosure document requirements.
- **Compliance Manual**: Comprehensive document containing firm's policies and procedures for meeting regulatory obligations.
- **Concentration Risk**: Risk arising from excessive exposure to single asset, sector, counterparty, or risk factor.
- **Conflicts of Interest**: Situations where firm's or individual's interests may compromise duty of loyalty or impartiality to clients.
- **Control Person**: Individual with authority to direct or cause direction of firm management or investment policy.
- **Counterparty**: Entity on opposite side of financial transaction including exchanges, broker-dealers, lenders, or smart contracts.
- **Counterparty Risk**: Risk that a counterparty will fail to meet its contractual obligations, including default, insolvency, or operational failure of exchanges, lenders, custodians, or other service providers.
- **Credit Risk**: Risk that counterparty will fail to meet obligations when due.
- **Currency Transaction Report (CTR)**: FinCEN-required report filed by financial institutions for currency transactions exceeding $10,000, documenting the transaction details and customer identification.
- **Custodian**: Entity legally responsible for safeguarding client assets with operational control over access and disposition.
- **Custody Rule**: SEC Rule 206(4)-2 requiring registered investment advisers with custody of client assets to maintain funds with qualified custodians, provide account statements, and undergo annual surprise examinations.
- **Customer Identification Program (CIP)**: Regulatory requirement under the Bank Secrecy Act for financial institutions to verify the identity of customers opening accounts, including collection and verification of name, date of birth, address, and identification number.
- **Decentralized Autonomous Organization (DAO)**: Organization governed by smart contract rules and token holder voting without centralized management.

- **Decentralized Exchange (DEX)**: Trading protocol enabling peer-to-peer cryptocurrency transactions through smart contracts without centralized intermediary.
- **Decentralized Finance (DeFi)**: Financial applications built on blockchain networks executing functions through smart contracts without traditional intermediaries.
- **Depeg**: Event where a stablecoin's market price deviates significantly from its intended peg value, creating potential losses for holders and systemic risks for protocols relying on price stability.
- **Digital Asset**: Cryptographically secured representation of value or rights recorded on distributed ledger or blockchain.
- **Directors and Officers (D&O) Insurance**: Liability insurance protecting individuals serving in governance or executive positions from personal losses.
- **Disaster Recovery Plan (DRP)**: Documented procedures for restoring technology systems, data, and operations following a disaster or major disruption, including recovery priorities, procedures, and testing requirements.
- **Disclosure**: Material information provided to clients or prospective clients regarding investment strategies, risks, fees, conflicts, or firm operations.
- **Drawdown**: Peak-to-trough decline in investment value during specific period.
- **Exposure Limit**: Maximum permitted exposure to a particular asset, sector, counterparty, or risk factor, established to control concentration risk and enforce risk appetite boundaries.
- **Failover**: Process of automatically or manually switching operations to backup systems, locations, or service providers when primary resources become unavailable.
- **Fair Value**: The price at which an asset would change hands between willing buyer and seller, neither under compulsion, with reasonable knowledge of relevant facts, used as the basis for portfolio valuation.
- **Fiat Currency**: Government-issued currency not backed by physical commodity (USD, EUR, GBP).
- **Fiduciary**: Person or entity holding legal duty to act in another's best interests with highest standard of care.
- **Financial Industry Regulatory Authority (FINRA)**: Self-regulatory organization overseeing broker-dealers and registered representatives.
- **Flash Loan**: Uncollateralized loan borrowed and repaid within single blockchain transaction.

- **Form ADV**: SEC registration form and disclosure document required of registered investment advisers.
- **Front Running**: Prohibited practice of executing trades ahead of client orders to benefit from anticipated price movement.
- **Funding Rate**: Periodic payment exchanged between long and short position holders in perpetual swap contracts to keep the contract price aligned with the underlying spot price.
- **Futures Commission Merchant (FCM)**: Entity registered with CFTC to solicit or accept orders for futures contracts.
- **Gas Fee**: Transaction cost paid to blockchain network validators for processing operations.
- **General Counsel**: Senior legal officer responsible for firm's legal affairs and compliance.
- **Governance Token**: Cryptocurrency token that grants holders voting rights on protocol decisions, parameter changes, treasury allocations, and other governance matters.
- **Gross Exposure**: Sum of absolute values of all long and short positions without netting.
- **Hard Fork**: Blockchain protocol change creating permanent divergence from previous version, potentially resulting in two separate chains.
- **Hardware Security Module (HSM)**: Physical computing device that safeguards and manages cryptographic keys, performs encryption and decryption, and provides tamper-resistant key storage for high-security applications.
- **Hardware Wallet**: Physical device storing cryptocurrency private keys offline.
- **Hedge**: Investment position intended to offset potential losses in another position.
- **Hot Wallet**: Cryptocurrency storage where private keys remain connected to internet-enabled systems for operational accessibility.
- **Impermanent Loss**: Temporary reduction in value when providing liquidity to automated market maker relative to holding underlying assets.
- **Incident Response Plan**: Documented procedures for detecting, responding to, containing, and recovering from security incidents or operational disruptions, including escalation protocols and communication procedures.
- **Independent Director**: Board member without material relationship to firm beyond directorship.

- **Insider Trading**: Illegal practice of trading securities based on material nonpublic information.
- **Institutional Investor**: Organization investing substantial assets including pension funds, endowments, foundations, insurance companies, and sovereign wealth funds.
- **Investment Adviser**: Person or entity compensated for providing investment advice or managing client assets.
- **Investment Committee**: Governing body responsible for reviewing and approving investment decisions, monitoring portfolio performance, ensuring adherence to investment policy, and providing oversight of the investment process.
- **Investment Policy Statement (IPS)**: Document defining investment objectives, constraints, strategies, and guidelines for portfolio management.
- **Key Management**: Processes and controls for generating, storing, backing up, and controlling access to cryptographic private keys.
- **Key Person Risk**: Operational risk arising from excessive dependence on specific individuals whose departure, incapacity, or unavailability would materially disrupt firm operations, investment management, or regulatory compliance.
- **Know Your Customer (KYC)**: Regulatory requirement to verify client identity and understand client circumstances before establishing relationship.
- **Layer 2 (L2)**: Secondary protocol built on top of a base blockchain (Layer 1) designed to improve scalability, reduce transaction costs, and increase throughput while inheriting security from the underlying chain.
- **Leverage**: Use of borrowed capital or derivatives to amplify investment exposure beyond available equity.
- **Limit Order**: Instruction to execute transaction at specified price or better.
- **Liquid Staking**: Providing cryptocurrency to staking protocol while receiving liquid token representing staked position.
- **Liquidation**: Forced closing of leveraged positions when collateral becomes insufficient to support obligations.
- **Liquidity**: Ability to convert asset to cash quickly without significant price impact.
- **Liquidity Pool**: Smart contract holding reserves of two or more tokens that enables automated trading through algorithmic pricing, with liquidity provided by users who earn fees in exchange for their deposits.
- **Liquidity Provider**: Entity supplying assets to trading venue or protocol to facilitate transactions.

- **Management Fee**: Ongoing fee charged by investment managers for portfolio management services, typically expressed as an annual percentage of assets under management.
- **Margin**: Collateral deposited to support leveraged position or derivative contract.
- **Margin Call**: Demand for additional collateral when position losses reduce margin below required minimum.
- **Mark-to-Market**: Valuation method that prices assets at current market prices based on observable transactions or executable quotes.
- **Market Maker**: Entity providing continuous bid and offer quotes to facilitate trading and provide liquidity.
- **Markets in Crypto-Assets (MiCA)**: European Union regulatory framework for crypto-asset service providers establishing licensing, capital, governance, and consumer protection requirements across EU member states.
- **Material Information**: Information that reasonable investor would consider important in making investment decision.
- **Miner Extractable Value (MEV)**: Profit blockchain validators can extract by including, excluding, or reordering transactions within blocks.
- **Multi-Party Computation (MPC)**: Cryptographic technique distributing private key generation and signing across multiple parties without reconstructing complete key.
- **Multi-Signature (Multisig)**: Wallet configuration requiring multiple private key approvals before executing transactions.
- **Net Asset Value (NAV)**: Per-share value calculated by dividing total net assets by outstanding shares.
- **Net Exposure**: The difference between long and short positions, representing directional market exposure after accounting for offsetting positions.
- **Netting**: Offsetting long and short positions to calculate net exposure.
- **Non-Disclosure Agreement (NDA)**: Contract prohibiting sharing confidential information with unauthorized parties.
- **Off-Chain**: Activities, data, or transactions occurring outside blockchain network.
- **Office of Foreign Assets Control (OFAC)**: U.S. Treasury Department office administering and enforcing economic sanctions programs, requiring screening of transactions and counterparties against sanctions lists.

- **Omnibus Wallet**: Single wallet address holding assets for multiple clients or accounts, requiring robust internal accounting and reconciliation to track individual ownership.
- **On-Chain**: Activities, data, or transactions recorded directly on blockchain network.
- **Operational Risk**: Risk of loss resulting from inadequate or failed internal processes, people, systems, or external events, including technology failures, human error, fraud, and business disruption.
- **Oracle**: Service providing external data to smart contracts executing on blockchain networks.
- **Over-the-Counter (OTC)**: Trading conducted directly between parties rather than through centralized exchange.
- **Performance Attribution**: Analysis decomposing portfolio returns into components attributable to different factors, decisions, or exposures to understand sources of performance relative to benchmarks.
- **Performance Fee**: Compensation based on investment returns, typically calculated as percentage of profits above specified threshold.
- **Perpetual Swap**: Derivative contract similar to futures but without expiration date, using funding rate mechanisms to maintain price alignment with the underlying spot market.
- **Politically Exposed Person (PEP)**: Individual holding prominent public position or function, or their close associates, requiring enhanced due diligence due to elevated corruption and money laundering risks.
- **Position Limit**: Maximum size of position permitted in a particular asset, instrument, or strategy, established to control concentration risk and ensure portfolio diversification.
- **Pricing Source**: Data provider or methodology used to determine asset valuations, including exchanges, data aggregators, index providers, or valuation models for illiquid assets.
- **Prime Broker**: Financial institution providing comprehensive services to investment managers including custody, financing, securities lending, and execution.
- **Private Key**: Cryptographic credential providing control over blockchain address and authority to authorize transactions.
- **Proof of Reserves**: Cryptographic verification demonstrating custodian controls assets claimed without revealing sensitive information.

- **Protocol Governance**: Decision-making processes and mechanisms through which decentralized protocols are managed, upgraded, and operated, typically involving token holder voting on proposals.
- **Protocol Risk**: Risk specific to blockchain protocols including smart contract vulnerabilities, governance attacks, oracle manipulation, economic exploits, and consensus mechanism failures.
- **Qualified Custodian**: Custodian meeting SEC Rule 206(4)-2 requirements including banks, registered broker-dealers, registered futures commission merchants, or qualifying foreign financial institutions.
- **Re-entrancy Attack**: Smart contract vulnerability where an external contract can repeatedly call back into the vulnerable contract before the first execution completes, potentially draining funds.
- **Reconciliation**: Process of comparing internal records against external statements from custodians, administrators, exchanges, or counterparties to identify and resolve discrepancies.
- **Recovery Point Objective (RPO)**: Maximum acceptable amount of data loss measured in time, defining how frequently data must be backed up to meet business continuity requirements.
- **Recovery Time Objective (RTO)**: Maximum acceptable duration for restoring systems or operations after a disruption, defining the target time for resuming critical functions.
- **Redemption**: Process by which investor withdraws capital from fund or separately managed account.
- **Registered Investment Adviser (RIA)**: Investment adviser registered with SEC or state securities authorities.
- **Regulatory Risk**: Risk that changes in laws, regulations, or regulatory interpretation materially impact business operations, investment strategies, or asset valuations.
- **Risk Appetite**: The level and types of risk an organization is willing to accept in pursuit of its objectives, typically documented in a board-approved risk appetite statement.
- **Risk Committee**: Board or management committee responsible for overseeing risk management framework, monitoring risk exposures, reviewing limit breaches, and ensuring alignment with risk appetite.
- **Risk Register**: Comprehensive inventory of identified risks including assessment of likelihood, impact, existing controls, and mitigation strategies for each risk.

- **Sanctions Screening**: Process of checking customers, counterparties, and transactions against OFAC and other sanctions lists to identify prohibited parties or jurisdictions.
- **Scenario Analysis**: Risk assessment technique examining portfolio impact under specific hypothetical events or market conditions, complementing statistical measures like VaR.
- **Securities and Exchange Commission (SEC)**: Federal agency regulating securities markets, investment advisers, and investment companies.
- **Segregated Wallet**: Dedicated wallet address holding assets for a single client or account, providing clear ownership separation and simplified reconciliation.
- **Segregation**: Separation of client assets from firm assets to prevent commingling and ensure client protection.
- **Segregation of Duties**: Internal control principle requiring different individuals to perform incompatible functions such as transaction initiation, approval, execution, and reconciliation to prevent fraud and errors.
- **Self-Custody**: Arrangement where client maintains direct control over private keys rather than delegating custody to third party.
- **Service Level Agreement (SLA)**: Contract defining expected service standards, performance metrics, and remediation rights.
- **Shamir's Secret Sharing**: Cryptographic technique that divides a secret (such as a private key) into multiple shares, requiring a threshold number of shares to reconstruct the original secret.
- **Slashing**: Penalty mechanism in proof-of-stake networks where validators lose staked assets for protocol violations.
- **Smart Contract**: Self-executing computer program deployed on blockchain network that automatically enforces agreement terms when specified conditions occur.
- **Smart Contract Audit**: Independent review of smart contract code to identify security vulnerabilities, logic errors, and potential exploits before or after deployment.
- **Smart Contract Risk**: Risk of loss from vulnerabilities, bugs, or exploits in smart contract code, including logic errors, re-entrancy attacks, and upgrade mechanism failures.
- **Stablecoin**: Cryptocurrency designed to maintain stable value relative to reference asset, typically U.S. dollar.

- **Staking**: Locking cryptocurrency in proof-of-stake network to support operations and earn rewards.
- **Stress Testing**: Analysis assessing portfolio resilience under extreme but plausible scenarios, including market crashes, liquidity crises, counterparty failures, and operational disruptions.
- **Sub-Custodian**: Third-party entity to which a primary custodian delegates physical custody or safekeeping of certain assets, creating additional counterparty relationships requiring due diligence.
- **Suitability**: Requirement that investment recommendations align with client's investment objectives, risk tolerance, and financial situation.
- **Suspicious Activity Report (SAR)**: FinCEN-required report filed by financial institutions when transactions appear to involve funds derived from illegal activity, lack business purpose, or otherwise suggest money laundering or other financial crimes.
- **Systematic Monitoring**: Regular, documented review process occurring at defined intervals without requiring triggering event.
- **Tail Risk**: Risk of rare but severe events occurring in the tails of probability distributions, representing losses significantly beyond normal market volatility.
- **Technology Risk**: Risk arising from technology systems including cybersecurity threats, system failures, data breaches, software vulnerabilities, and technology obsolescence.
- **Time-Lock**: Smart contract mechanism that delays execution of certain functions for a specified period, providing time for review and potential intervention before irreversible actions occur.
- **Total Value Locked (TVL)**: Aggregate value of cryptocurrency assets deposited in a DeFi protocol, used as a metric for protocol adoption, liquidity depth, and potential systemic importance.
- **Travel Rule**: Regulatory requirement for financial institutions to transmit originator and beneficiary information with fund transfers exceeding certain thresholds, extended to cryptocurrency transactions by FinCEN and FATF guidance.
- **Validator**: Network participant in proof-of-stake blockchain responsible for verifying transactions and creating new blocks.
- **Valuation Committee**: Governance body responsible for overseeing asset valuation policies, reviewing pricing methodologies, resolving valuation disputes, and approving fair value determinations for complex or illiquid assets.

- **Value at Risk (VaR)**: Statistical measure estimating maximum potential loss over specified time period at given confidence level.
- **Wallet**: Software or hardware interface for storing private keys and interacting with blockchain networks.
- **Warm Wallet**: Cryptocurrency storage where private keys remain online but behind additional security layers including multi-signature requirements or hardware security modules.
- **Waterfall**: Sequence defining priority of distributions from fund or investment structure.
- **Whitelisting**: Security control restricting transactions or access to pre-approved addresses, accounts, or entities.
- **Yield Farming**: Strategy of deploying cryptocurrency across DeFi protocols to maximize returns through lending, liquidity provision, staking rewards, and token incentives.

ENDNOTES

- Almeida, J., and T.C. Gonçalves. "A Systematic Literature Review of Volatility and Risk Management on Cryptocurrency Investment." *MDPI Risks Journal*, 2022. https://www.mdpi.com/2227-9091/10/5/107
- Alternative Investment Management Association (AIMA). "AIMA Publishes Fund Manager Code of Conduct (FMCC) Implementation Guide." October 2018. https://www.aima.org/article/aima-publishes-fund-manager-code-of-conduct-fmcc-implementation-guide.html
- Alternative Investment Management Association (AIMA). "AIMA Publishes New Guide on Digital Asset Trading." May 10, 2023. https://www.aima.org/article/press-release-aima-publishes-new-guide-on-digital-asset-trading.html
- Alternative Investment Management Association (AIMA). "AIMA Updates Its Guide to Sound Practices for Investor Relations." November 25, 2024. https://www.aima.org/article/aima-updates-its-guide-to-sound-practices-for-investor-relations.html
- Alternative Investment Management Association (AIMA). "AIMA's Policy Principles." https://www.aima.org/regulation/aima-s-policy-principles.html
- Alternative Investment Management Association (AIMA). "Digital Assets & Anti-Money Laundering." October 5, 2022. https://www.aima.org/event/digital-assets—anti-money-laundering.html
- Alternative Investment Management Association (AIMA). "Guide to Sound Practices for the Valuation of Investments." 2018. https://www.sec.gov/comments/s7-07-20/s70720-7464497-221255.pdf
- Alternative Investment Management Association (AIMA). "Guides to Sound Practices." https://www.aima.org/sound-practices/guides-to-sound-practices.html
- Alternative Investment Management Association (AIMA). "Integrating Your Digital Assets Technology Stack with the Traditional Asset Manager Operating Model." September 23, 2024. https://www.aima.org/journal/aima-journal—edition-139/article/integrating-your-digital-assets-technology-stack-with-the-traditional-asset-manager-operating-model.html
- Alternative Investment Management Association (AIMA). "Investor Relations: An AIMA Guide to Sound Practices." https://www.aima.org/compass/practical-guides/marketing-investor-relations/investor-relations.html

- Alternative Investment Management Association (AIMA). "Digital Asset Trading: An AIMA Industry Guide." May 2023. https://www.aima.org/compass/insights/digital-assets/digital-asset-trading.html
- arXiv. "Quantifying Crypto Portfolio Risk: A Simulation-Based Framework." July 2025. https://arxiv.org/html/2507.08915v1
- BitGo. "Crypto Custody for Hedge Funds: Security and Compliance." July 10, 2025. https://www.bitgo.com/resources/blog/crypto-custody-for-hedge-funds-security-compliance-and-growth-strategies/
- BitGo. "Crypto Disaster Recovery: Safeguarding Your Digital Assets." July 24, 2025. https://www.bitgo.com/resources/blog/crypto-disaster-recovery/
- California Law Review. "Applying the SEC Custody Rule to Cryptocurrency Hedge Fund Managers." https://www.californialawreview.org/print/applying-the-sec-custody-rule-to-cryptocurrency-hedge-fund-managers
- CFA Institute. "Asset Manager Code of Professional Conduct." 2019. https://www.cfainstitute.org/en/ethics-standards/codes/asset-manager-code
- CFA Institute. "Elements of an Investment Policy Statement for Institutional Investors." https://rpc.cfainstitute.org/sites/default/files/-/media/documents/article/position-paper/investment-policy-statement-institutional-investors.pdf
- CFA Institute. "Global Investment Performance Standards (GIPS)." 2020 ed. https://www.cfainstitute.org/en/ethics-standards/codes/gips-standards
- CFA Institute. "Global Investment Performance Standards (GIPS) Handbook." 2nd ed., 2007. https://www.gipsstandards.org/wp-content/uploads/2021/03/gips_handbook_2nd_edition.pdf
- CFA Institute. "Investment Management Governance." https://rpc.cfainstitute.org/policy/positions/investment-management-governance
- CFA Institute. "Portfolio Management: An Overview." October 3, 2025. https://www.cfainstitute.org/insights/professional-learning/refresher-readings/2025/portfolio-management-overview
- CFA Institute. "Standard VI(A) Avoid or Disclose Conflicts." Updated January 2024. https://www.cfainstitute.org/standards/professionals/code-ethics-standards/standards-of-practice-vi-a
- Collas Crill. "Crypto-Asset Investment Structures: A Primer." January 30, 2025. https://www.collascrill.com/articles/crypto-asset-investment-structures-a-primer/

- Cornell Law School. "17 CFR § 275.206(4)-7 - Compliance procedures and practices." https://www.law.cornell.edu/cfr/text/17/275.206(4)-7
- Cyber Risk Institute (CRI). "The CRI Profile: A Financial Sector Use Case for the NIST CSF." 2024. https://cyberriskinstitute.org/wp-content/uploads/2024/05/The-CRI-Profile-A-Financial-Sector-Use-Case-for-the-NIST-CSF-2023.pdf
- Deloitte. "2025 Investment Management Regulatory Outlook." https://www.deloitte.com/us/en/services/consulting/articles/investment-management-regulatory-outlook.html
- Deloitte. "Lessons in Digital Asset Risk Management." 2025. https://www.deloitte.com/us/en/services/audit-assurance/articles/blockchain-digital-assets-risk-management.html
- DLA Piper. "CFTC updates guidance on compliance programs and enforcement." https://www.dlapiper.com/en-us/insights/publications/2020/09/cftc-updates-guidance-on-compliance-programs-and-enforcement
- European Securities and Markets Authority. "Alternative Investment Fund Managers Directive (AIFMD)." Directive 2011/61/EU, June 8, 2011. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0061
- European Securities and Markets Authority. "Markets in Crypto-Assets Regulation (MiCA)." Regulation (EU) 2023/1114, June 9, 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114
- European Systemic Risk Board. "Systemic liquidity risk: a monitoring framework." https://www.esrb.europa.eu/pub/pdf/reports/esrb.report202501_systemicliquidityrisk~90f2044791.en.pdf
- EY Parthenon. "2025 Institutional Investor Digital Assets Survey: Growing Enthusiasm Propels Digital Assets into the Mainstream." March 18, 2025. https://www.ey.com/content/dam/ey-unified-site/ey-com/en-us/insights/financial-services/documents/ey-growing-enthusiasm-propels-digital-assets-into-the-mainstream.pdf
- Fabozzi, Frank J. *Hedge Funds: Structure, Strategies, and Performance*. Hoboken, NJ: John Wiley & Sons, 2004
- Federal Reserve Bank of New York. "The Financial Stability Implications of Digital Assets." *Economic Policy Review*, November 2024. https://www.newyorkfed.org/research/staff_reports/sr1034

- Financial Action Task Force. "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." Updated October 2021. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf
- Financial Action Task Force. "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation." Updated October 2023. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf
- Financial Conduct Authority (UK). "FCA Handbook: Conduct of Business Sourcebook (COBS)." https://www.handbook.fca.org.uk/handbook/COBS/
- Financial Conduct Authority (UK). "Guidance on Cryptoassets." Policy Statement PS19/22, July 31, 2019. https://www.fca.org.uk/publication/policy/ps19-22.pdf
- Financial Crimes Enforcement Network. "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies." FIN-2019-G001, May 9, 2019. https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf
- Financial Crime Academy. "The Power Of Compliance: AML Regulations For Cryptocurrency Unleashed." https://financialcrimeacademy.org/aml-regulations-for-cryptocurrency/
- Financial Professionals Organization. "10 Treasury Policies Every Company Should Have." April 14, 2025. https://www.financialprofessionals.org/training-resources/resources/articles/Details/10-treasury-policies-every-company-should-have
- Financial Stability Board. "Assessment of Risks to Financial Stability from Crypto-assets." February 16, 2022. https://www.fsb.org/wp-content/uploads/P160222.pdf
- Financial Stability Board. "Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets." July 17, 2023. https://www.fsb.org/wp-content/uploads/P170723-2.pdf
- Fintech Global. "How to prepare for the 2025 Form ADV update: key compliance tips." https://fintech.global/2025/03/12/how-to-prepare-for-the-2025-form-adv-update-key-compliance-tips/
- Fireblocks. "Addressing counterparty risk with Fireblocks Off Exchange." https://www.fireblocks.com/blog/addressing-counterparty-risk-and-unlocking-new-opportunities-with-fireblocks-off-exchange/
- Fireblocks. "Digital Asset Custody and Transaction Processing Leading Practices Using Fireblocks' MPC Solution." June 28, 2025.

https://www.fireblocks.com/report/digital-asset-custody-and-transaction-processing-leading-practices-using-fireblocks-mpc-solution/

- Fireblocks. "Disaster Recovery Services: A New Standard for Digital Asset Security." March 21, 2025. https://www.fireblocks.com/blog/disaster-recovery-services-new-standard-digital-asset-security/
- Fireblocks. "Mitigating digital asset and crypto counterparty risk." https://www.fireblocks.com/blog/mitigating-digital-asset-and-crypto-counterparty-risk/
- Fireblocks. "What Is Digital Asset Custody?" https://www.fireblocks.com/digital-asset-custody/
- Fordham Law Review. "Protecting Investors from Hedge Fund Managers' Conflicts of Interest." https://ir.lawnet.fordham.edu/flr/vol77/iss6/9/
- Fund Associates. "Sound Practices for Hedge Fund Managers." https://www.fundassociates.com/sound-practices/
- Galaxy Digital. "A Risk Rating Framework for DeFi and Crypto Investors." 2025. https://www.galaxy.com/insights/research/risk-rating-defi-crypto
- Global Association of Risk Professionals (GARP). "Digital-Asset Risk Management: VaR Meets Cryptocurrencies." October 18, 2024. https://www.garp.org/risk-intelligence/market/digital-asset-risk-241018
- Global Reporting Initiative. "GRI Standards." 2021. https://www.globalreporting.org/standards/
- Government Finance Officers Association (GFOA). "Investment Policy." https://www.gfoa.org/materials/investment-policy
- Government Finance Officers Association (GFOA). "Treasury and Investment Management Best Practices." https://www.gfoa.org/best-practices/treasury-operations
- Greenberg Traurig. "Federal Banking Regulators Issue Guidance on Risk Management for Crypto-Asset Safekeeping Activities." 2025. https://www.gtlaw.com/en/insights/2025/7/federal-banking-regulators-issue-guidance-on-risk-management-for-crypto-asset-safekeeping-activities
- Guizot, Armelle. *The Hedge Fund Compliance and Risk Management Guide*. Hoboken, NJ: John Wiley & Sons, 2006
- Harvard Law School Forum on Corporate Governance. "Hedge Fund Governance." https://corpgov.law.harvard.edu/2013/04/15/hedge-fund-governance/

- Hedge Fund Law Report. "How Can Hedge Fund Managers Structure Managed Accounts." https://www.pelawreport.com/2678721/how-can-hedge-fund-managers-structure-managed-accounts-to-remain-outside-the-purview-of-the-amended-custody-rules-surprise-examination-requirement.thtml
- Hedge Fund Law Report. "Key Person Provision Drafting and Legal Requirements." 2025. https://www.hflawreport.com/key-person-provision-drafting-legal-requirements/
- Hunton Andrews Kurth. "SEC and CFTC Propose Digital Asset Reporting on Form PF." https://www.hunton.com/blockchain-legal-resource/sec-and-cftc-propose-digital-asset-reporting-on-form-pf
- International Monetary Fund. "Global Financial Stability Report: Digital Money Across Borders." October 2023. https://www.imf.org/en/Publications/GFSR/Issues/2023/10/10/global-financial-stability-report-october-2023
- International Organization for Standardization. "ISO/IEC 27001:2013 Information Security Management Systems." 2013. https://www.iso.org/standard/54534.html
- International Organization for Standardization. "ISO/IEC 27002:2022 Information Security Controls." 2022. https://www.iso.org/standard/75652.html
- International Organization of Securities Commissions. "Policy Recommendations for Crypto and Digital Asset Markets." May 2023. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD734.pdf
- International Organization of Securities Commissions. "Principles for Financial Market Infrastructures." April 2012. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD377.pdf
- IRS. "Form 1023: purpose of conflict of interest policy." https://www.irs.gov/charities-non-profits/form-1023-purpose-of-conflict-of-interest-policy
- Journal of Community Development Research. "Blockchain-based Risk Management Framework for Digital Asset Exchanges: Bridging COSO ERM with Emerging Technologies." 2025. https://so18.tci-thaijo.org/index.php/JCDR-HS/article/view/807
- Keiter CPA. "2025 Digital Asset Reporting | Form 1099-DA." https://keitercpa.com/blog/new-digital-asset-tax-reporting-regulations-2025/

- Kim, C.Y., and K. Lee. "Risk Management to Cryptocurrency Exchange and Investors: Guidelines to Prevent Potential Threats." IEEE Conference on Platform Technology and Service, 2018
- Kitces. "Guide To Documenting Annual Compliance Review: SEC Amendment." https://www.kitces.com/blog/annual-compliance-review-sec-investment-adviser-written-requirements-rule-20647/
- Kleinberg Kaplan. "Preserving A Hedge Fund's Business and Legacy - The Keys to A Robust Succession Plan." https://www.kkwc.com/wp-content/uploads/2017/08/Preserving-A-Hedge-Fund%E2%80%99s-Business-and-Legacy-The-Keys-to-A-Robust-Succession-Plan-Hedge-Fund-LCD.pdf
- Managed Funds Association. *Sound Practices for Hedge Fund Managers*. 2009 ed. Washington, D.C.: MFA, 2009
- Managed Funds Association. "Sound Practices for Hedge Fund Managers." https://www.cftc.gov/sites/default/files/idc/groups/public/@swaps/documents/file/soundpractices.pdf
- Merkle Science. "Counterparty Risk in Crypto: Understanding the Potential Threats." https://www.merklescience.com/counterparty-risk-in-crypto-understanding-the-potential-threats
- Merkle Science. "What is Counterparty Analysis." https://www.merklescience.com/what-is-counterparty-analysis-and-how-does-it-apply-to-crypto-companies
- Mishcon de Reya. "Crypto and the FATF 'travel rule'." https://www.mishcon.com/news/crypto-and-the-fatf-travel-rule
- Mondrian Alpha. "The Evolution of Quantitative Risk Management in Hedge Funds." https://www.mondrian-alpha.com/articles/investment/quantitative-risk-management
- Morris, Peter J. T. *All About Hedge Funds: The Easy Way to Get Started*. New York: McGraw-Hill, 2004
- National Institute of Standards and Technology. "Cybersecurity Framework Version 1.1." April 16, 2018. https://www.nist.gov/cyberframework
- National Institute of Standards and Technology (NIST). "The NIST Cybersecurity Framework (CSF) 2.0." February 26, 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

- NBER. "HEDGE FUND LEVERAGE." https://www.nber.org/system/files/working_papers/w16801/w16801.pdf
- NYU Compliance & Enforcement. "Proposed SEC Custody Rules for Crypto Assets." https://wp.nyu.edu/compliance_enforcement/2023/03/16/proposed-sec-custody-rules-for-crypto-assets/
- Office of the Comptroller of the Currency. "Interpretive Letter 1170 on Crypto-Asset Custody Services." 2020. https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf
- Office of the Comptroller of the Currency. "OCC Clarifies Bank Authority to Engage in Crypto-Asset Custody and Execution Services." May 7, 2025. https://www.occ.gov/news-issuances/news-releases/2025/nr-occ-2025-42.html
- Office of the Comptroller of the Currency, Federal Reserve, and FDIC. "Agencies Issue Joint Statement on Risk-Management Considerations for Crypto-Asset Safekeeping." July 14, 2025. https://www.occ.gov/news-issuances/news-releases/2025/nr-ia-2025-68.html
- Office of the Comptroller of the Currency, Federal Reserve, and FDIC. "Crypto-Asset Safekeeping by Banking Organizations." July 14, 2025. https://www.occ.gov/news-issuances/news-releases/2025/nr-ia-2025-68a.pdf
- Paul, Weiss. "Private Funds Regulatory Compliance Calendar 2025." https://www.paulweiss.com/media/cgskoxtn/private_funds_regulatory_compliance_calendar_2025.pdf
- PLANSPONSOR. "Managing Counterparty Risk More Important for Hedge Funds Now." https://www.plansponsor.com/managing-counterparty-risk-more-important-for-hedge-funds-now/
- Principles for Responsible Investment. "Responsible Investment Due Diligence Questionnaire for Hedge Funds." 2020. https://www.unpri.org/hedge-funds/responsible-investment-ddq-for-hedge-funds/4544.article
- Principles for Responsible Investment. "The Six Principles for Responsible Investment." 2006. https://www.unpri.org/about-us/what-are-the-principles-for-responsible-investment
- Professional Risk Managers' International Association. "PRM Handbook: A Comprehensive Guide to Current Theory and Best Practices in Risk Management." 2004. https://www.prmia.org/

- PwC. "6th Annual Global Crypto Hedge Fund Report." https://www.pwc.com/gx/en/industries/financial-services/crypto-services/sixth-annual-global-crypto-hedge-fund-report.html
- Reich, J., and M. Gilman. "Setting the Standards Blog Series: Part 1 — The Foundation of Fund Administration for Digital Assets." MG Stover, 2023. https://www.mgstover.com/news/setting-the-standards-blog-series-part-1-the-foundation-of-fund-administration-for-digital-assets
- Richey May & Co. "Unique Valuation Considerations for Crypto Asset Managers." 2024. https://richeymay.com/resource/whitepapers/unique-valuation-considerations-for-crypto-asset-managers/
- Shadab, Houman B. "Hedge Fund Governance." *Stanford Journal of Law, Business & Finance* 19, no. 1 (Fall 2013): 141–202. https://digitalcommons.nyls.edu/fac_articles_chapters/1037
- Sidley. "Crypto-Focused Private Fund Adviser Settles with U.S. SEC for Custody Rule and Other Violations." https://www.sidley.com/en/insights/newsupdates/2024/09/crypto-focused-private-fund-adviser-settles-with-us-sec-for-custody-rule-and-other-violations
- Soni, U., and R.G. Preece. "Valuation of Cryptoassets: A Guide for Investment Professionals." CFA Institute Research and Policy Center, 2023. https://rpc.cfainstitute.org/research/reports/2023/valuation-cryptoassets
- Standards Board for Alternative Investments (SBAI). "Alternative Investment Standards." 2020. https://www.sbai.org/standards/
- Standards Board for Alternative Investments (SBAI). "Culture and Diversity Principles." 2024. https://www.sbai.org/asset/A13A3BFA-2771-4F42-AD55B07E9694914E/
- Standards Board for Alternative Investments (SBAI). "Cyber Security (Small & Mid-Size Firms)." https://www.sbai.org/static/bdcd6b3b-bb90-49b7-b5835c2d4de4d3e9/Cyber-Security-small-&-mid-size-firms.pdf
- Standards Board for Alternative Investments (SBAI). "Governance." https://www.sbai.org/toolbox-resources/governance.html
- Standards Board for Alternative Investments (SBAI). "Investment DD and the Standards." https://www.sbai.org/resource/investment-dd-and-the-standards.html
- Standards Board for Alternative Investments (SBAI). "Operational Due Diligence of Digital Assets." November 2021. https://www.sbai.org/static/5e928706-402a-43da-a036b82c6a7fd8c6/Operational-Due-Diligence-on-Digital-Assets.pdf

- Standards Board for Alternative Investments (SBAI). "Responsible Investment Policy Framework." 2024. https://www.sbai.org/static/dfcb3593-d5fb-4b9e-b761fd8bca67968b/Responsible-Investment-Policy-Framework.pdf
- Standards Board for Alternative Investments (SBAI). "Responsible Investment Toolbox Resources." 2024. https://www.sbai.org/toolbox-resources/responsible-investment.html
- Standards Board for Alternative Investments (SBAI). "Standardised Board Agenda." https://www.sbai.org/static/373e2aa6-b543-4041-bc3bc83f72816741/Standardised-Board-Agenda.pdf
- State Street. "Digital Digest July 2025: Digital Asset Custody." July 2025. https://www.statestreet.com/cn/en/insights/digital-digest-july-2025-digital-asset-custody
- Sustainability Accounting Standards Board. "SASB Standards for Asset Management & Custody Activities." 2023. https://www.sasb.org/standards/materiality-finder/
- Talos. "Bridging the Liquidity Gap: How Digital Asset Infrastructure Is Rising to Meet Institutional Demands." September 29, 2025. https://www.talos.com/insights/bridging-the-liquidity-gap-how-digital-asset-infrastructure-is-rising-to-meet-institutional-demands
- Talos. "Nasdaq Trade Talks: The Pace of Institutional Adoption of Digital Assets." https://www.talos.com/insights/the-pace-of-institutional-adoption-of-digital-assets
- The Hedge Fund Journal. "A Seven-Step Guide to Effective Business Continuity Planning." https://thehedgefundjournal.com/a-seven-step-guide-to-effective-business-continuity-planning/
- The Hedge Fund Journal. "Business Continuity for Hedge Fund Managers." https://thehedgefundjournal.com/business-continuity-for-hedge-fund-managers/
- The Hedge Fund Journal. "Counterparty Exposure Risk." https://thehedgefundjournal.com/counterparty-exposure-risk/
- The Hedge Fund Journal. "IT Considerations for Disaster Recovery." https://thehedgefundjournal.com/it-considerations-for-disaster-recovery/
- The Hedge Fund Journal. "Managing Potential Conflicts of Interest." https://thehedgefundjournal.com/managing-potential-conflicts-of-interest/

- The Hedge Fund Journal. "Risk Practices in Hedge Funds." https://thehedgefundjournal.com/risk-practices-in-hedge-funds/
- Troutman Pepper. "Digital Asset Regulation and The CLARITY Act of 2025." https://www.troutman.com/insights/digital-asset-regulation-and-the-clarity-act-of-2025.html
- Trustpair. "Wire Transfer Fraud: Definition, Strategies and Recovery." June 30, 2025. https://trustpair.com/blog/wire-transfer-fraud-prevention-best-practices-and-recovery/
- U.S. Congress. "GENIUS Act - Federal Regulatory Framework for Stablecoins." Signed into law July 18, 2025. https://www.congress.gov/committee-report/119th-congress/house-report/94/1
- U.S. Department of the Treasury. "Action Plan for Addressing Illicit Financing Risks of Digital Assets." September 2022. https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf
- U.S. Department of the Treasury. "Financial Management Standards." August 21, 2025. https://tfx.treasury.gov/fm-standards
- U.S. Securities and Exchange Commission. "Compliance Programs of Investment Companies and Investment Advisers." https://www.sec.gov/rules-regulations/2003/12/compliance-programs-investment-companies-investment-advisers
- U.S. Securities and Exchange Commission. "Crypto Asset Exchange-Traded Products Disclosure Requirements." 2025. https://www.sec.gov/newsroom/speeches-statements/cf-crypto-asset-exchange-traded-products-070125
- U.S. Securities and Exchange Commission. "Crypto Asset Custody By Investment Advisers After The SEC's Proposed Safeguarding Rule." https://www.sec.gov/about/crypto-task-force/crypto-task-force-written-input/ctf-written-rscr-walker-03222023
- U.S. Securities and Exchange Commission. "Custody of Funds or Securities of Clients by Investment Advisers." 17 CFR § 275.206(4)-2. https://www.sec.gov/rules/final/ia-2176.htm
- U.S. Securities and Exchange Commission. "Digital Asset Securities." Staff Accounting Bulletin No. 121, March 31, 2022. https://www.sec.gov/oca/staff-accounting-bulletin-121

- U.S. Securities and Exchange Commission. "Framework for 'Investment Contract' Analysis of Digital Assets." April 3, 2019. https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets
- U.S. Securities and Exchange Commission. "Interpretive Matters Concerning Independent Directors of Investment Companies." https://www.sec.gov/rules-regulations/1999/10/interpretive-matters-concerning-independent-directors-investment-companies
- U.S. Securities and Exchange Commission. "Investment Advisers Act of 1940 – Section 206(4) / Rule 206(4)-3." https://www.sec.gov/divisions/investment/noaction/2019/wells-fargo-securities-032119-2064
- U.S. Securities and Exchange Commission. "Office Hours with Gary Gensler: What is a Qualified Custodian." https://www.sec.gov/newsroom/speeches-statements/office-hours-gary-gensler-qualified-custodian
- U.S. Securities and Exchange Commission. "Role of Independent Directors of Investment Companies." https://www.sec.gov/rules-regulations/2001/01/role-independent-directors-investment-companies
- Unchained. "What Is Counterparty Risk in Crypto?" https://unchainedcrypto.com/counterparty-risk-in-crypto/
- University of Cambridge. "Cambridge Centre for Alternative Finance: 2nd Global Cryptoasset Regulatory Landscape Study." 2024. https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-cryptoasset-regulatory-landscape-study/

ABOUT THE DFSB

The Digital Fiduciary Standards Board (DFSB) is an independent, nonprofit standards-setting organization established to advance operational maturity in digital asset investment management. Through open, transparent standards development, DFSB provides allocators with a consistent framework for evaluating manager operational quality, managers with a practical roadmap to institutional credibility, and regulators with evidence of industry self-governance.

For more information, visit www.dfsb.org.

DFSB
DIGITAL FIDUCIARY STANDARDS BOARD