The Importance of Risk Due Diligence in Cryptocurrency Strategy, Investing and Rebounding

Cryptocurrency has continued to face tremendous scrutiny, and recent events have underscored the pitfalls that can arise when risk due diligence is overlooked or lacks rigor. Future investors and business leaders engaging in the cryptocurrency industry can take lessons learned from past missteps to implement a more robust and risk-based approach to assess opportunities and investments in the digital assets space. This article outlines the key elements of strong due diligence for risk management drawing on long-standing theory in traditional finance combined with requirements specific to this space.

Over the past year, it's become clear across global markets just how important risk management and governance are to mitigating fraud and protecting large capital investments.

Companies seeking investment may position their focus on risk management as diligent and prudent, though early-stage and high-growth companies often grow faster than their risk controls can keep up. For investors, failure to take a detailed assessment of governance and processes can lead to devastating losses and/or severe legal and regulatory liability. Conversely, with early, effective and ongoing due diligence, many potential risks can be caught before they spiral into catastrophe.

Just as in traditional financial markets, key risk management questions that should be asked for investments in the digital assets arena will examine controls and performance across governance, operational risk, credit risk, market risk and third-party risk.

Governance

Growing companies often speak of the "institutionalization" of their business and being on a path to build out infrastructure and controls as they mature. The key question is whether they have matured enough by the time they are seeking substantial capital and holding high values of customer funds. Many young companies do not appoint committees or leaders of compliance, cybersecurity or risk in their formative years, but rather build out risk management capabilities over time.

Ideally any organization that is backed by or responsible for large sums of money will have a chartered management-level risk committee in place. Such a committee should meet at least monthly and review exposures, evaluate emerging risks and vote on key issues. Meetings should be recorded and subjected to effective review and challenge by senior management, and separately, the board of directors.

A lack of formal policy or procedures should be viewed as a significant red flag. Entities may try to "check the box" by producing poorly organized and ineffective policies or producing a document that simply mirrors a regulatory guidance letter with no real internalization of the rules. In contrast, sophisticated entities will have thoughtful risk management policies and procedures that are tailored and right sized for their business. The best will maintain an inventory of management controls tied to identified risks and referenced in policy and procedures, with specified owners, categorization, trigger events and response requirements including documentation.

At the very least, there should be evidence that processes were carried out. This includes minutes of monthly meetings and ongoing risk reporting summarizing quantified exposures such as market and credit risk. On the operational risk side, organizations should produce incident reporting logs summarizing material loss events and near-misses.

Operational Risk and Controls

Controls segregating customer assets from company assets, as well as internal controls, accounting and recordkeeping best practices must be implemented and enforced.

One challenge in approaching the term "operational risk" is that it encompasses a widely disparate range of exposures and vulnerabilities. Cybersecurity and information security, financial crime risks, data governance and data privacy risks, technology risks, accounting risk, transaction processing risk, HR risks, physical risks and others fall under the broad rubric of operational risk. Administering an effective operational risk capability is a challenge that requires a wide range of experts, program coordination, sophisticated documentation and reporting.

Transaction processing risk in particular entails a much different range of vulnerabilities in a crypto-native firm than in a traditional capital markets firm. Procedures governing wallet and wire operations should have controls that ensure assets are only sent to whitelisted wallet destinations (and definitely not to wallets on any global sanctions lists). Custody, whether in-house or through third-party custodians, should use multi-party computation ("MPC") or multi-signature approval protocols, and ideally should require individual transaction approvers to use multi-factor authentication ("MFA") or other protections. Use of third parties can mitigate some of these risks, but in turn create third-party risk exposures.

Organizations should have a head of compliance responsible for "Know Your Customer" ("KYC") and anti-money laundering ("AML") controls and related compliance, and a chief information security officer responsible for cybersecurity. In addition to these key leaders, there must also be stakeholders who can provide independent review and challenge across other business activities that may create risk.

The first area to review controls is related to management of customer funds and assets. The company should be able to demonstrate the effectiveness of its controls enforcing securities laws and the customer terms of service, particularly with respect to segregation of customer assets.

Emails and messaging chats likely need to be retained in accordance with federal, state and local laws, especially when transaction requests are approved via these channels. The company's risk management function should periodically review the content of emails and chats, and also assess that messaging processes are not taking place that increase operational risk.

Accounting capabilities and financial statements should be audited by a reputable audit firm. Inter-company transfers and related-party transactions should be properly controlled, recorded and disclosed in accounting records. AML and KYC controls should be independently assessed. Ongoing AML transaction monitoring should be governed by policy, evidenced with documentation, and ideally, independently validated.

Cybersecurity and information leakage risks require a deep-dive assessment of their own, but to start, entities should be able to identify the full-time staff dedicated to those risks, the depth of their experience, and the degree of their expertise with digital assets. If the entity had any material hack or breach event in its history, it should be able to demonstrate it responded to the event and refined its risk management processes as a result.

Credit Risk

A key question due diligence processes often miss is concentration risk: if the largest loan a company made defaulted, and any collateral posted turned out to be worth much less than expected, what would be the residual capitalization of the company? What if the largest three loans defaulted?

A key characteristic of credit risk in this space is that borrowers principally bear market risk to earn revenue. Lending to such entities therefore requires depth in both credit risk and market risk. The crypto world can take key long-standing lessons from the TradFi world on this front. Large borrowers must be required to provide complete portfolio data and related risk metrics to lenders. Our teams have seen cases first hand where opaque portfolio Net Asset Value (NAV) reports were provided that later turned out to have been well overstated.

A centralized finance ("CeFi") entity should be able to clearly articulate key features of its credit risk management function, such as limits at the portfolio and single-name level, its due diligence questionnaire, the types of materials it requires from potential borrowers and how it verifies representations made. Specifically, it should demonstrate active review and challenge of claims made by its borrowers as to their revenue model and strategic positioning, and the composition and fair valuation of assets provided as collateral.

Updated assessments documented with periodic reviews (*i.e.*, call reports) should be generated at regular intervals and in response to any key headline that could impact creditworthiness. The master lending agreement should confer rights to review corporate books and record of borrowers, conduct on-site visits and request updated materials when conditions have clearly changed, and lenders should demonstrate that they availed themselves of those rights in relevant circumstances.

A loophole that can exist in credit risk processes is a lack of rigorous controls on changes to the terms and conditions of existing loans. The same governance and approval processes followed for initial loans should also apply to subsequent upsizing, extensions, changes in collateral, amendments, waivers or other material changes to terms and conditions.

Market and Liquidity Risk

Market observations have illustrated that many CeFi entities' revenue models were built around long (bullish) exposure to digital assets.

A key question in assessing market and liquidity risk is determining whether an entity's P&L exhibits leveraged exposure to the prices of digital assets over time. If yes, how much imputed exposure to alt-coins is observed relative to Bitcoin or Ethereum? The entity should know its exposure to alt-coins and blue chips and generally have limits on alt-coin exposure. Revenue derived from staking and related risks should be clearly reported, particularly if third-party staking services are used. It should regularly run a stress test that evaluates residual capitalization in the face of a severe drawdown, perhaps 50% or more, in a basket of key digital assets and have that information readily available.

P&L drivers should be clearly articulated, and specifically whether a large portion of earnings is derived from principal trading activity that is unlikely to be sustainable.

Given the current high-volatility interest rate environment, investors must conduct rigorous quantification of liquidity buffers and evaluation of the company's ability to cover expenses during extended periods of zero cash inflows.

Third-Party Risk

As rapidly growing companies, CeFi entities often rely on third parties to satisfy a wide range of needs including technology, data, security, professional services, administrative services and workplace/experience providers, among others. These practices can introduce large third-party risk exposure, all of which must be understood and addressed by senior management.

A company should be able to readily identify its largest third-party dependencies and understand the implications that a failure by any of them would create for the overall enterprise risk profile. The most common risk exposures caused by third-party failures are operational resilience, regulatory compliance, API technology support and cyber/information security. Any major failure event at a third party should be reviewed by the company, with specific remediation steps identified and implemented.

If the entity is large enough, full-time staff devoted to third-party risk may be appropriate. Leading entities will have policy and procedures documentation, specific tracking of key performance indicators and key risk indicators, and related management reporting.

Perspective and Opinion

At the peak of the last crypto cycle in November 2021, The Block identified 64 crypto "unicorns," companies with valuations exceeding $1 billion.[1] While in some sense the rapid run-up in valuations in CeFi and other parts of the digital assets industry demonstrates the strength and dynamism of financial markets to efficiently direct capital to the most exciting opportunities, it also calls for attention to risk. When demand exists to invest in a hot area, risk management may take a back seat to meeting that demand. Business leaders must be vigilant about this and uphold strong standards for governance and due diligence, even in the face of rapid growth and industry hype.

As an industry, the goal within digital assets should be to identify a common language of due diligence and minimum standards that are being met pre-close before capital is put at risk, and in developing more active ongoing monitoring of investments.

It's also important to note that while there are often commonalities in risk profiles, any specific case might involve unique situational risk. The next time an exciting investment opportunity arises, whether that be something new in the blockchain and digital asset space or beyond, investors and business leaders must include a deep-dive into risk management capabilities in their due diligence, which will ultimately benefit the industry, investors and consumers.

[1] Wilhelm, Alex, "*As crypto unicorns multiply, the US stands out as ground zero for blockchain winners*", TechCrunch, November 19, 2021, https://techcrunch.com/2021/11/19/as-crypto-unicorns-multiply-the-us-stands-out-as-ground-zero-for-blockchain-winners/

PAUL FELDMAN
Senior Director
+1 212 499 3687
paul.feldman@fticonsulting.com

FRANCK RISLER
Senior Managing Director
+1 212 841 9348
franck.risler@fticonsulting.com

JACO SADIE
Senior Managing Director
+1 415 283 4230
jaco.sadie@fticonsulting.com

JOSE CEPEDA
Senior Managing Director
+1 212 499 3645
jose.cepeda@fticonsulting.com

JAMES BALCOM
Senior Managing Director
+1 212 841 9356
james.balcom@fticonsulting.com

STEVE MCNEW
Senior Managing Director
+1 713 353 5404
steve.mcnew@fticonsulting.com

11082023 | VN02773-v05