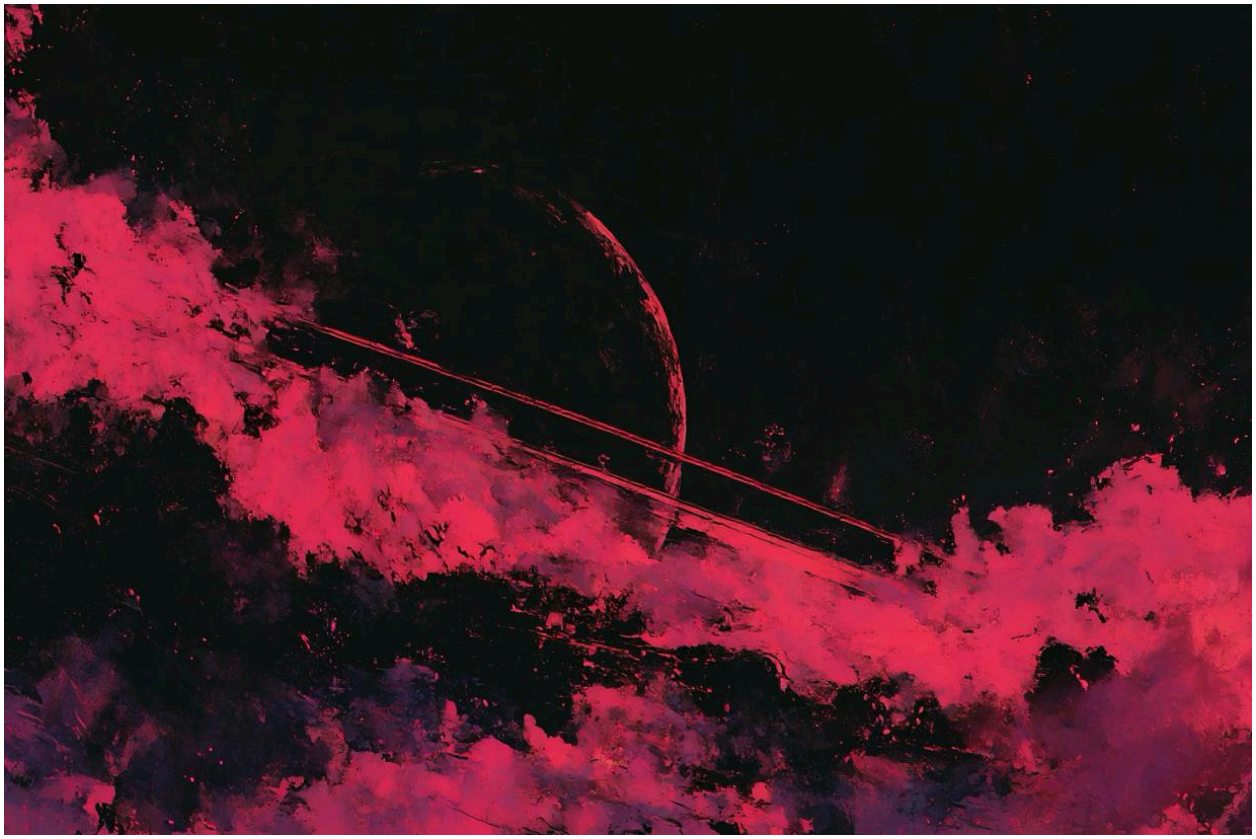

A FRAMEWORK FOR INSTITUTIONAL CRYPTO SECURITY

Immunefi

PUBLISHED DATE 3/Oct/2025

SOURCE IMMUNEFI

THE STATE OF INSTITUTIONAL SECURITY

Digital Asset Treasuries (DATs) are emerging as one of the most important institutional vehicles for holding and deploying cryptocurrency at scale. In 2025 alone, they have attracted over $20 billion in venture funding underscoring the speed and scale of their rise.

Unlike exchange-traded funds (ETFs), which primarily track baskets of assets, DATs differentiate themselves by actively putting assets to work. They stake, lend, and deploy capital into DeFi protocols and real-world asset (RWA) platforms, enabling them to generate higher yields than what ETFs can typically provide today.

This opportunity comes with risk. While custody of reserves is largely solved by third-party custodians, the real exposure begins once assets leave the custodian's vault and enter staking contracts, liquidity pools, or lending protocols. These deployments can fail through smart contract vulnerabilities, governance attacks, liquidity crises, or ecosystem contagion. For DATs, the challenge is not simply achieving yield, but doing so in a way that demonstrates disciplined risk management to investors, regulators, and the broader market.

The core question is one of confidence. Can DATs show that their strategies expand the yield frontier without taking on reckless risk? To succeed, they need to be able to assess the security of the protocols they deploy to, monitor their exposures in real time, and actively contribute to strengthening the ecosystems that underpin their returns. Security is not just operational; it is a market signal that separates disciplined institutional products from speculative experiments.

This paper sets out a framework for how DATs can manage these risks and position themselves as the credible, resilient alternative to ETFs: delivering higher yields while proving they can do so safely.

HOW TO USE THIS FRAMEWORK

This framework is designed as a practical playbook for DATs. It can be applied in three phases that build on one another:

1. **Baseline controls:** Establish custody oversight, clear governance roles, and robust operational security posture. These measures form the foundation on which more advanced practices depend.
2. **Protocol due diligence and monitoring:** Move beyond custody to the real differentiator: how capital is deployed. Apply structured risk scoring, continuous monitoring, and deployment criteria that treat protocols like institutional counterparties.
3. **Co-investment and continuous assurance:** Mature DATs do not just consume security, they invest in it. By co-funding audit competitions and bug bounty programs, and monitoring for the protocols they rely on, DATs signal to investors that yield is generated within ecosystems that are constantly tested and reinforced.

Taken together, these phases allow DATs to show not only that they manage risk, but that they do so in a way investors, regulators, and markets can verify.

WHAT ARE THE SECURITY RISKS FOR DATS?

The risks facing Digital Asset Treasuries are not confined to the vaults of custodians. Those are secure, regulated, and already hardened. The real exposures begin once assets are deployed into external environments. DATs generate their returns by staking, lending, and participating in DeFi protocols or tokenized markets, which means they inherit the risks of those ecosystems. Failures can occur in four places: through custodial dependencies, internal governance lapses, vulnerabilities in the protocols where capital is deployed, and the broader market and regulatory environment.

This section outlines those domains of risk. Each carries distinct dynamics, yet all converge on the same point: investor confidence depends on whether DATs can show that yield is pursued with discipline, not recklessness.

2.1. Custody oversight

DATs typically do not manage private keys directly. Reserves sit with regulated third-party custodians that provide hardened infrastructure, regulatory compliance, and continuous monitoring. This removes many of the direct risks often discussed in retail or DAO contexts, such as hot wallet compromises or mismanaged seed phrases.

Outsourcing, however, does not eliminate risk. Custodians themselves become a point of concentration, where weaknesses in governance, software, or jurisdictional alignment can cascade into systemic exposure. For example, a custodian domiciled in one jurisdiction may be compelled by regulators or courts to freeze or repatriate assets regardless of the wishes of the DAT or its investors. Insurance coverage is similarly uneven, often capped well below the scale of institutional reserves and riddled with exclusions. The reliance on a third party introduces

dependencies that need to be scrutinized with the same seriousness as any other element of the reserve framework.

For DATs, the strategic question is not whether to use custodians, since that choice is effectively settled, but how to oversee them. Independent validation of custodian governance, adversarial testing of operational controls, and structured incident response planning provide signals of discipline to markets and regulators. Immunefi's Professional Services can support this need through governance reviews, independent validation of key management frameworks, and operational security assessments, with a focus on areas such as MPC implementation and escalation procedures. These mechanisms allow DATs to demonstrate to investors that custody arrangements are not simply delegated but continuously challenged and verified.

2.2 Operational oversight

Custodians manage the technical perimeter of reserves, but DATs remain accountable for the human and procedural systems that govern how those reserves are accessed, deployed, and reported. Operational failures have been the root cause of many of the largest collapses in the digital asset ecosystem, even where custody arrangements were intact. Weak governance, unclear escalation paths, or misaligned incentives can transform isolated incidents into systemic crises.

The gap for DATs lies in governance clarity and incident preparedness. Many organizations still operate with diffuse accountability, where no single role is empowered to act decisively during emergencies. This lack of ownership creates delays that are fatal in blockchain environments where transactions are irreversible. Equally problematic is the absence of tested incident response frameworks. Without rehearsed escalation paths, a breach can metastasize from a technical compromise into a reputational and financial crisis that undermines investor confidence.

DATs should embed operational oversight as a matter of institutional design. This includes defining clear role-based authority for reserve-related actions, formalizing onboarding and offboarding procedures for individuals with privileged access, and maintaining incident response plans that are treated as doctrine rather than contingency. Independent red-team exercises and operational audits are vital tools in this process.

Through specialized partners, Immunefi delivers structured simulations and adversarial reviews that expose latent weaknesses in escalation, communication, and decision-making. By adopting these practices, DATs not only reduce the likelihood of operational failure but also demonstrate to investors and regulators that governance is treated with the same seriousness as custody and infrastructure.

2.3 Protocol deployment risk

For DATs, the distinctive risk does not lie in custody or infrastructure managed by third parties, but in how reserves are deployed into external protocols. Yield generation through staking, liquidity provision, or participation in decentralized finance is a major differentiator for DATs. It is also where they face their greatest exposure. Every deployment introduces dependency on smart contracts, governance systems, and ecosystems that are outside the DAT's direct control.

The gap lies in the absence of reliable, consistent standards for assessing protocol security. Today, most projects rely on one-off audits, security certifications of varying depth, or informal reputation in the community. While these may provide surface-level reassurance, they offer little assurance at institutional scale, where continuous validation, structured scoring, and transparent criteria are needed. Without such standards, institutions are left comparing protocols in ad hoc ways, making it difficult to justify deployment decisions to investors, regulators, or risk committees.

A RUBRIC FOR PROTOCOL RISK

To evaluate protocols at institutional scale, DATs need a consistent scoring framework. Key dimensions include:

- **Audit assurance:** Number and diversity of audits completed, recency of those audits, and whether independent audit competitions have been conducted to pressure-test findings.
- **Bug bounty coverage:** Whether the protocol has a live, adequately-funded bug bounty program (BBP) that creates continuous adversarial pressure, and how quickly past submissions have been resolved.
- **Continuous monitoring:** Whether onchain activity and security signals are being monitored in real time for anomalies, governance exploits, or liquidity manipulation.
- **Ongoing adversarial and operational testing:** Ongoing adversarial testing: Evidence that the protocol invests in continuous reviews beyond audits, including bug bounty programs, audit competitions, threat modeling, and operational security audits.
- **Liquidity resilience (secondary):** Still relevant, but assessed alongside security posture since shallow liquidity often compounds exploit impact.
- **Ecosystem security dependencies:** Whether the protocol relies on upstream or downstream projects that themselves lack strong security practices (audits, BBPs, monitoring).
- **Exploit response maturity:** How a protocol has historically responded to disclosures or exploits, speed, transparency, and whether fixes were independently validated.

This provides a basis for consistent evaluation and comparison, allowing DATs to demonstrate to investors that protocol selection is disciplined, transparent, and repeatable.

To manage this risk, DATs need to approach protocol deployment with the same rigor that traditional institutions apply to counterparties. This means structured risk scoring of smart contracts, continuous onchain monitoring, and clear criteria for acceptable exposure. Immunefi provides full-spectrum safeguards including Audits, Audit Competitions, Bug Bounty Programs, Onchain Monitoring, and PR reviews, each designed to surface vulnerabilities before they become systemic risks. Together, these measures offer DATs and institutional stewards the ability to validate protocol resilience continuously rather than relying on static, point-in-time assessments.

DATs can further strengthen their position by both co-investing in and demanding stronger security from the protocols they use, acting more like activist shareholders who tie their liquidity provision to clear expectations of resilience. This proactive stance not only protects reserves but signals to investors that yield is pursued through disciplined risk management rather than opportunism.

2.4 Market and macro risk

Beyond technical and operational exposures, DATs face risks from the broader market and regulatory environment. These risks are not unique to DATs, but they determine whether reserves can function under stress and whether investors continue to view DATs as credible, disciplined managers.

The most immediate concern is liquidity. Assets that appear liquid in normal conditions can become illiquid in moments of market stress, leaving DATs unable to exit positions without steep discounts. For organizations that promise stability and responsiveness, the inability to access reserves at critical moments undermines credibility.

Volatility compounds this challenge. Digital assets can lose significant value in short timeframes, eroding the effectiveness of reserves as stabilizing instruments. While some level of volatility is inherent, unmanaged exposure to high-beta assets can leave DATs vulnerable to sudden shocks that investors interpret as poor risk discipline.

Regulatory and taxation shifts create persistent uncertainty. A digital asset that appears compliant today may be reclassified tomorrow, particularly through the regulatory treatment of exchanges or custodians that list it, exposing DATs to unexpected legal or financial obligations.More importantly, these shifts alter investor confidence. Institutions that anticipate and prepare for regulatory change signal discipline. Those caught unprepared appear reckless and undermine their case for institutional trust.

Macro risks are not purely financial events. They intersect directly with security. Liquidity crunches can trigger large-scale withdrawals that strain network capacity or stress-test protocol infrastructure, creating operational instability even if underlying security is intact. Volatility can amplify incentives for adversaries to exploit weaknesses during market stress. Regulatory shifts can suddenly make previously safe deployment strategies high-risk.

Market and macro dynamics must be integrated into the security framework, not treated as separate concerns. Security teams and risk officers should collaborate on liquidity stress testing, diversified exposure policies, and regulatory foresight. Combined with external validation, these measures signal that yield is balanced by resilience and that reserves can withstand shocks.

WHAT SECURITY SOLUTIONS SHOULD DATS EMPLOY?

Identifying risks is not enough. DATs need to also show how they will manage them with frameworks that are visible, repeatable, and trusted. Security for a DAT is not a technical checklist but a market signal, it demonstrates to investors and regulators that higher yields are supported by mature governance and continuous oversight.

This section sets out the practices and mechanisms DATs can adopt across five layers: custody oversight, operational governance, protocol deployment, market resilience, and organizational security. Each layer strengthens the others, and each is an opportunity to prove that yield is earned responsibly. Alongside the principles, we highlight where Immunefi contributes independent validation, adversarial testing, and monitoring that help DATs meet institutional standards.

3.1. Custody oversight and validation

Regulated third-party custodians already safeguard DAT reserves. They operate hardened infrastructure and enforce compliance frameworks. The task for DATs is independent validation and ongoing oversight so delegation does not become blind trust.

Custodian failures are rare, but the concentration of authority they represent makes oversight essential. Jurisdictional pressures can compel custodians to restrict or repatriate assets regardless of investor intent. Insurance provisions, while common, often fall short of institutional scale and exclude many forms of loss. Even with regulated providers, governance gaps, operational blind spots, or geopolitical dependencies can have systemic consequences.

DATs should adopt a model of independent validation. Use adversarial testing of operational procedures, structured reviews of custody governance structures (including MPC and multisig where relevant), and continuous monitoring of custodian processes. These measures do not duplicate the custodian's job. They prove to investors and regulators that custodians are held to the highest standard.

HOW IMMUNEFI HELPS:

- Immunefi Treasury Protect provides expert custody governance reviews (covering multisig and MPC setups as relevant), ensuring custodian processes are continuously validated.
- Immunefi IR Preparedness Program delivers tabletop exercises, live simulations, and playbooks to test readiness under stress

Through these measures, DATs can demonstrate to investors that reserves are not only entrusted to custodians but also subject to independent, continuous validation. This oversight transforms custody from a dependency into a signal of discipline and maturity.

3.2 Operational governance

Custodians safeguard the assets, but operational preparedness over how those assets are deployed remains the DAT's responsibility. Across the industry, collapses have often been linked to poor incident readiness and escalation. For DATs, the risk lies not in governance gaps but in ensuring that processes and preparedness match institutional standards.

The core challenge is readiness. While DATs already operate with clear governance and fiduciary structures, escalation chains and incident response plans must be tested and continuously updated. Blockchain settlement finality magnifies the need for speed: once a transaction is executed, it cannot be reversed. Preparedness ensures decisive action under pressure.

DATs already operate with strong governance; what they must elevate is preparedness. This means ensuring reserve deployment and emergency response are supported by tested escalation paths, robust onboarding/offboarding protocols, and incident response plans that are rehearsed, documented, and capable of functioning under pressure.

HOW IMMUNEFI HELPS:

- Red Team Simulations expose gaps in escalation and communication by simulating real-world breaches.
- Incident Response Coverage provides immediate, expert support when critical events occur.
- vCISO Services bring senior security leadership into DATs without requiring full in-house teams, aligning security with board-level priorities, enforcing policy discipline, and ensuring incident readiness.

By embedding these practices, DATs transform operational governance into a form of systemic resilience. Investors see not only that assets are custodied securely, but that the organization itself is designed to withstand stress without collapsing into disorder.

3.3 Protocol deployment security

DATs do not simply hold assets; they deploy them to generate yield. This creates a new layer of exposure that custodians do not cover. Every smart contract, governance system, and ecosystem they touch becomes part of the DAT's risk perimeter.

The gap is the lack of standardized, institutional-grade ways to evaluate protocol risk. One-off audits and reputational signals are insufficient for institutions deploying billions. Without structured evaluation, DATs expose investors to risks that look like opportunism rather than disciplined management.

DATs need to adopt systematic approaches to protocol risk. That means: risk scoring frameworks that assess code, governance, and economic design; continuous monitoring to detect anomalies or governance exploits; and clear deployment criteria that set thresholds for exposure and conditions for withdrawal.

HOW IMMUNEFI HELPS:

- Bug Bounty Programs and Audit Competitions create continuous adversarial pressure that goes beyond one-time audits.
- PR Reviews assess technical risks before capital is deployed.
- Onchain Monitoring provides real-time visibility into anomalies that could signal compromise.

By embedding protocol deployment security, DATs can credibly show investors that yield is generated through discipline, not chance. This reframes protocol exposure from a liability into a competitive advantage

3.4 Market and liquidity resilience

Use prescriptive controls to neutralize market fragility. Build defenses for volatility, liquidity crunches, and counterparty failure so stress events do not force value-destructive moves. Investors read these controls as evidence of disciplined management.

Under stress, assets that are liquid in normal times can freeze, leaving DATs unable to exit without steep losses. Volatility can erode reserves just when stability is needed most. Counterparty collapses show how contagion can wipe out value even when the underlying asset seems sound.

DATs need to prove they anticipate these conditions, not react late. That means: liquidity stress testing to model exit scenarios; diversified exposure that avoids concentration in thin markets; counterparty reviews that go deeper than audits; and predefined rebalancing rules that trigger automatically when thresholds are crossed.

HOW IMMUNEFI HELPS:

- Independent security validation of counterparties and infrastructure resilience (e.g., exchanges, custodians, smart contracts)
- Continuous monitoring for technical failures that could exacerbate financial stress
- Clear delineation of scope: While liquidity and volatility are financial risks, Immunefi ensures that security failures do not compound them.

By embedding these measures, DATs show investors that yield is balanced with resilience. The ability to withstand stress without panic selling or loss of confidence sets them apart as disciplined managers rather than speculators.

3.5 Organizational security posture

The decisive layer of protection for DATs is organizational. Cryptography and infrastructure may be strong, but failures in identity, personnel, or institutional discipline can still compromise reserves. Investors and regulators judge the credibility of a DAT as much by its organizational maturity as by its returns. Weak posture here signals fragility, while strong posture demonstrates that yield is pursued responsibly, at institutional standards.

Weak identity controls, insecure devices, and untrained staff create attack surfaces for adversaries. Insider risk is just as critical: people with privileged access are prime targets for coercion or recruitment, especially when large sums are at stake. Without strong personnel security, even the best custody or infrastructure models are exposed.

Data should build organizational resilience across four dimensions:

- Identity and access management: Strict role separation, strong authentication, universal hardware-based 2FA, and continuous monitoring of privileged accounts to prevent hijacking or misuse.
- Device and endpoint security: Laptops, phones, and servers hardened, patched, and monitored with enterprise-grade EDR, with automated containment and rapid response. DATs must also run phishing simulations and endpoint compromise drills, since staff devices are often the weakest link.
- Personnel vetting and monitoring: Background checks, financial reviews, insider risk programs, and ongoing monitoring for sensitive roles. Personnel are the highest-value targets for adversaries, making this discipline critical.
- Incident readiness: Predefined escalation paths, tabletop simulations, and recovery playbooks to ensure resilience under attack.

HOW IMMUNEFI HELPS:

- Immunefi OpSec Audit hardens organizational security posture through employee/device hygiene reviews, phishing simulations, and tailored roadmaps.
- Immunefi vCISO delivers fractional executive security leadership and Magnus-integrated security governance, and can help set up EDR.
- Immunefi Incident Response provides 24/7 expert-led exploit response, exchange coordination, and recovery playbooks.

For DATs, organizational posture is not merely hygiene, it is a market signal. It proves that yield is managed under enterprise discipline, not opportunism. This strengthens investor trust, improves regulator confidence, and sets DATs apart from less mature actors.

CONCLUSION

DATs represent a new stage in digital asset adoption. By deploying capital into staking, DeFi, and tokenized markets, they can deliver returns that ETFs cannot. The advantage holds only with visible discipline. Without credible security frameworks, higher yields look like reckless exposure rather than a competitive edge.

The challenge now is everything after custody: selecting secure protocols, monitoring exposures in real time, ensuring liquidity under stress, and operating with robust governance. Trust is built or lost in these arenas.

The solution is integration. Security must operate as a continuous system that combines protocol risk assessment, monitoring, organizational discipline, and financial resilience. The DATs that win will run this system with institutional discipline.

Immunefi supports this standard. Protocol assessments, continuous onchain monitoring, and professional services strengthen governance and operations. Co-investment in protocol security lets DATs show prudence and leadership, turning yield into a credible, investable strategy.

The future of DATs will be determined by who manages risk most visibly and effectively. With the right posture, DATs unlock new use cases, earn investor trust, and help position digital assets as a stable pillar of institutional finance.