1inch Risk Management

Building a Risk Management Framework for Decentralized Finance

Abstract

Decentralized finance has shown that non-custodial, permissionless systems can deliver efficient execution, deep liquidity access, and composable financial primitives at global scale. As these systems increasingly underpin real economic activity, the central question is no longer whether DeFi works, but how it remains resilient, credible, and trustworthy as complexity and impact grow.

1inch Shield represents a risk management architecture apt to be embedded directly at the infrastructural and protocol level of decentralized systems. Rather than relying on custody, identity-based controls, or retrospective enforcement, Shield integrates risk awareness into protocols and applications themselves—operating at transaction speed and within user-authorized constraints. It combines contextual analysis, multi-source intelligence, behavioral and environment signals, and coordinated incident response to reduce risk precisely when value moves.

This paper presents 1inch's approach to risk management as a native system design. It describes the architectural choices, operational governance, and ecosystem coordination that support Shield today, and outlines how these mechanisms extend to meet the demands of increasingly sophisticated, infrastructure-grade decentralized finance.

The framework described in this paper reflects design principles and operational approaches that may evolve as decentralized infrastructure and risk-management techniques continue to develop. Descriptions are intended to illustrate how risk awareness can be embedded into protocol environments and should not be interpreted as exhaustive descriptions of internal controls or operational procedures.

1. From Execution Excellence to Risk Averse Maturity

Decentralized finance emerged under constraints fundamentally different from traditional financial systems. It prioritized non-custodial execution, open composability, and permissionless access over centralized control or identity-based safeguards. Today, decentralized finance is no longer experimental. DeFi systems routinely support complex routing, intent-based execution, and cross-protocol coordination, and are increasingly relied upon as shared financial infrastructure. As these systems underpin broader adoption, including emerging use cases such as tokenized real-world assets, the expectations placed on them shift

accordingly. Reliability, resilience, and integrity become baseline requirements.

Risk management, in this context, is not a corrective measure imposed from outside the ecosystem. It is a natural extension of industry maturity. When a decentralized system operates at global scale and machine speed, security and risk management must function as infrastructure: embedded into protocols and applications, continuously active, and capable of operating in real time.

This challenge is inherent to DeFi's design philosophy. Traditional security models rely on account control, identity verification, or custodial intervention – approaches DeFi cannot adopt without compromising its core properties: user sovereignty, privacy, and permissionless access.

The framework described in this paper reflects our belief that robust risk discipline in decentralized finance is both possible and necessary. At 1inch, risk management—encompassing infrastructural security, integrated risk intelligence, and enterprise-grade governance—is encapsulated under 1inch Shield. This approach represents a best-in-class model in DeFi today, not by asserting control, but by aligning risk management with the autonomy- and privacy-first foundations of decentralization. Throughout this paper, "1inch Shield" refers to this framework.

2. 1inch Infrastructure, In Brief

1inch is a blockchain-based, permissionless routing infrastructure. It observes liquidity across protocols, computes execution paths under user-defined constraints, and routes signed instructions for on-chain execution without taking positions or exercising discretionary control. Understanding how security considerations propagate through infrastructure requires attention to the 1inch architecture.

1inch does not act as a custodian, broker, or counterparty. Execution is authorized exclusively through user-signed transactions and constrained by user-defined parameters; where those parameters cannot be met, transactions revert atomically on-chain.

Interaction within 1inch unfolds across several layers:

- **Web Layer**: User interface that allows access to aggregation and execution logic.
- **App Layer**: Self-custodial wallet with embedded on-chain interaction features
- **API Layer**: Programmatic access for integrators and institutional participants interacting with routing and execution infrastructure at scale.

Across all layers, execution follows the same model: users initiate and authorize transactions, while infrastructure coordinates it without taking custody or exercising discretionary control. These design choices define how execution is constructed, validated, and enforced across the system, and they shape how risk management mechanisms—including 1inch Shield—are integrated directly into transaction flows rather than applied externally.

3. Risk Management Across Layers

In decentralized finance, the risk control system does not reside in a single layer or control point. It emerges, or fails, across the entire system: user behavior and self-custody practices, interfaces and

wallets, execution infrastructure, protocols, liquidity sources.

Some risks are inherent to self-custody. Lost keys, compromised seed phrases, and social-engineering attacks depend primarily on user behavior and education, and no decentralized platform can fully eliminate them without undermining user autonomy. Other risks, however, arise from how execution itself unfolds: which contracts are touched, which assets and liquidity are involved, how interactions propagate across venues and time, and how adversarial actors exploit speed, composability, and fragmentation.

For this reason, 1inch commits to operating a risk framework at execution speed across layers through:

- Persistent risk detection, including ongoing monitoring, transaction analysis and on-chain simulation.
- Cross-surface signal correlation, combining on-chain data with device-, network-, and behavior-based indicators to identify patterns beyond individual wallets.
- Asset- and contract-level intelligence, covering malicious tokens, impersonation, and exploit-linked code.
- Policy-governed safeguards and escalation processes, enabling proportionate responses such as warnings, restrictions, or further review depending on context.
- Coordinated incident response, supported by continuous collaboration with specialized security partners and, where appropriate, relevant authorities.
- User-facing transparency and education, ensuring risks are surfaced at the point of execution rather than discovered after the fact.

The objective is not to control interactions, but to respond quickly enough to meaningfully reduce impact—while preserving decentralization and user agency.

4. 1inch Shield Risk Architecture

Risk management within decentralized infrastructure requires controls that are proportionate, transparent, and compatible with non-custodial system design. The 1inch Shield framework is structured to meet these objectives by embedding risk awareness across multiple interaction surfaces and intelligence sources while preserving user autonomy and permissionless access.

1inch Shield operates as a layered risk architecture embedded across protocol and execution infrastructure. Rather than relying on a single control point, data source, or enforcement mechanism, Shield is built around three reinforcing dimensions: multiple interaction surfaces, multiple independent intelligence sources, and multiple actors that materially influence outcomes. Signals are continuously re-evaluated as conditions evolve, allowing responses to remain flexible, reversible, and aligned with decentralized design principles.

4.1. Multi-Surface Risk Screening

Risk screening and assessment occur across multiple interaction surfaces within the 1inch ecosystem, each offering different visibility into trading behavior and context.

- **Front-end interfaces** provide the earliest opportunity to surface risk, at

the point where transaction intent is formed. Shield integrates geo-restrictions, real-time wallet screening, network-level signals (such as VPN or proxy detection where applicable), and user-facing risk warnings directly into transaction preparation and simulation flows.

- **API and integrator access** applies risk assessment to programmatic execution. Requests submitted by integrators, liquidity providers, and institutional systems are evaluated based on wallet behavior, transactional patterns, and execution context, without relying on a single enforcement point.
- **Call-data constructing infrastructure** provides both system-level visibility and active controls across execution. In addition to continuous on-chain analytics and anomaly detection, additional screening and risk checks are embedded directly into infrastructural components.
- **Governance and escalation surface** translates risk signals into coordinated response. Internal escalation procedures tie address- and profile-level risk scores, behavioral indicators, and execution context to predefined response paths, including automated actions, manual review, override, or coordinated incident response.

4.2. Multi-Source Risk Intelligence

At the core of Shield is a multi-source risk intelligence layer that aggregates, normalizes, and correlates inputs from a broad range of independent data providers or databases (public and coordinated blocklists) and data snapshots. These sources differ in scope, methodology, and signal type, and are intentionally combined to avoid reliance on any single feed or classification.

To achieve this, Shield organizes intelligence inputs into several functional categories, each contributing a distinct perspective on risk.

(a) Wallet and Actor Screening

Shield applies continuous screening to wallets and counterparties involved in transactions to assess exposure to sanctions, illicit activity, and high-risk behavioral patterns.

- Screening providers such as TRM Labs contribute sanctions and transaction risk intelligence used within the framework to help inform risk assessments related to users and counterparties.[1]
- This screening is enriched with contextual attribution and metadata from Etherscan (including Etherscan Pro), which provides address labels, contract metadata, and known associations.[2]

In addition to primary screening providers, Shield integrates a broad set of blocklists and intelligence sources that feed into 1inch's internal blocklist framework:[3]

- Industry war rooms and coordinated response groups, where industry leaders share validated indicators and

[1] TRM Labs (2024). *The 1inch Network Identifies Hundreds of High-risk Addresses* [Case Study]. TRM Labs. https://www.trmlabs.com/resources/case-studies/1inch-network-identifies-hundreds-of-high-risk-addresses
[2] See *Etherscan Pro documentation*, https://docs.etherscan.io/resources/pro-endpoints (docs.etherscan.io).
[3] See *Section 6.2*, where the cooperation with the providers and partners mentioned herein is covered in greater detail.

flagged addresses during active incidents.
- Ecosystem coordination channels, including SEAL-911 and Crypto ISAC, which distribute indicators of compromise and threat-actor patterns.
- Security partners such as ZeroShadow and InnerWorks, which contribute exploit-related indicators, behavioral signals, and maintained blocklists.
- Public issuer disclosures, including restricted or blocked address lists published by entities such as Circle and Tether.
- Crowdsourced intelligence, arising from blockchain transparency and community reporting by independent researchers, investigators, and watchdog initiatives, which 1inch treats as an early-warning signal subject to internal validation. Crystal Intelligence historical wallet screening data snapshot, that remains actively referenced as new behavior emerges.[4]

Impact:

- Risk decisions do not hinge on any single provider or list.
- When multiple signals align, a risk-averse default applies: execution is blocked.

(b) Transaction and Execution Screening

Transaction and execution screening serve to assess the concrete effects of a proposed interaction before it is finalized or propagated. Blockaid provides deterministic transaction simulation and validation, evaluating contract logic, approval scopes, asset flows, and execution outcomes prior to broadcast.[5] Simulations allow to identify unsafe or deceptive execution paths (exploit-linked interactions, malicious contract behavior, and unexpected asset movements) before a user signs or a transaction is routed. Broader market patterns and behavioral signals may also inform risk analysis in certain contexts. These analytical approaches are discussed further in Section 6.4.

Impact:

- Screening outcomes may surface as user-facing warnings during transaction simulation or influence routing behavior directly where elevated risk is detected.
- Responses are applied at execution time and do not alter user-signed instructions or assert custody over assets.

(c) Token and Asset Screening

Asset-level screening evaluates the tokens and contracts involved in transactions, recognizing that risk often originates from asset behavior rather than transaction structure alone.

- Web3 Antivirus is one of the providers supporting token and contract screening within Shield.[6] It detects malicious smart contracts, exploit-linked assets, embedded phishing logic, and UI-level attack patterns associated with token

[4] See *Crystal Intelligence's platform*: https://demo.crystalintelligence.com

[5] 1inch (2024), *1inch partners with Blockaid to finalize the Shield API,* 20 June 2024, 1inch Blog, https://blog.1inch.com/1inch-partners-with-blockaid-to-finalize-the-shield-api/

[6] 1inch (2025), *1inch beefs up its token warning system, 31 July 2025, 1inch Blog, https://blog.1inch.com/1inch-unveils-a-token-warning-system/*

interactions. This screening helps surface risks that may not be apparent from on-chain behavior alone, such as contracts designed to deceive users through interface-driven manipulation.
- Where applicable, this screening is complemented by Blockaid, which supports identification of malicious assets.

Impact:

- Execution and user experience are informed by asset-level risk.
- Warnings may be surfaced at the point of interaction where elevated risk indicators are identified.
- In certain cases, the framework may apply protective interaction restrictions for assets that present significant risk indicators.

(d) Interface and Domain Intelligence

1inch Shield extends screening to the interfaces and domains through which users initiate interactions.

- Tools provided by Blockaid support scanning to help identify malicious websites, compromised decentralized applications, and unsafe domains at the moment of connection. This includes identifying interaction flows or messages that embed malicious links or domains, enabling risks to be surfaced prior to transaction construction.
- Interface protection is further strengthened through collaboration with Phishfort, which scans the web for phishing campaigns, fake content, and brand impersonation related to 1inch interfaces.[7]
- Additional Web3-specific phishing intelligence is incorporated from providers such as ChainPatrol[8] which monitors malicious domains and scam campaigns targeting decentralized applications and wallet users.
- The automated monitoring is complemented by reports from the 1inch support team and ecosystem contributors, enabling faster identification and takedown of active scams.

Impact:

- Reduced exposure to fraudulent interfaces and deceptive access points.

(e) User, Device, and Environment Signals

The layered screening architecture described above enables Shield to incorporate user, device, and environment signals that extend risk assessment beyond addresses in isolation.

Probabilistic device fingerprints, network and VPN indicators, emulator and spoofing detection, and behavioral interaction patterns support detection of repeated abuse, automation, or evasion across wallets and sessions, without relying on identity, and in a manner consistent with DeFi's privacy expectations. The use of these signals is described in more detail in Section 5.

[7] See *PhishFort platform*: https://phishfort.com
[8] *See Chainpatrol platform:* https://chainpatrol.com/

4.3. Multi-Actor Risk Application

Shield's risk architecture is designed to apply across all actors that materially influence interaction, not solely end users. Screening and risk assessment are therefore applied consistently to:

- **Liquidity providers** (resolvers, solvers, market makers), are subject to continuous screening and manual assessment of their operational safeguards, risk-management practices, and observed behavior.
- **Developers and partners integrating 1inch API solutions** are subject to the same operational and behavioral assessments, with the addition of direct automatic restrictions on the wallet flags level.
- **Users and wallets** initiating execution may be subject to continuous, automated screening across address-, behavior-, and environment-level signals. Where risk thresholds are met, interaction is blocked by default and execution does not occur.

5. Beyond Addresses: Device Fingerprints and Behavioral Signals

Address-level screening is a non-negotiable baseline in decentralized environments. On its own, however, it is insufficient. Wallets can be created instantly and at no cost, and sophisticated actors routinely distribute activity across multiple addresses, chains, or sessions to evade detection. In such settings, risk often manifests not in a single address, but through repeated, coordinated, or automated patterns.

To address this, 1inch Shield extends risk assessment beyond addresses considered in isolation, correlating technical, environmental, and behavioral signals that are intrinsic to decentralized interaction itself. These signals may be grouped into privacy-preserving data clusters that provide continuity across activity without attempting to deanonymize users or construct identity-based representations.

This capability is supported by InnerWorks, which supplies device- and environment-level intelligence purpose-built for non-custodial systems. Shield incorporates technical and environmental signals that help identify patterns of automated, coordinated, or evasive activity across decentralized interactions. These signals are evaluated probabilistically and in combination with other contextual indicators. The objective is not to attribute identity, but to better distinguish organic user behavior from activity patterns that may present elevated risk.

For example, the framework may identify patterns where multiple wallets exhibit highly similar interaction behavior or execution timing that is inconsistent with typical user activity. Signals of this nature may inform further analysis or protective measures within the execution environment.

This approach allows the system to recognize coordinated or automated activity patterns without relying on identity-based controls or compromising the privacy expectations inherent in decentralized systems.

A combination of available signals operates probabilistically: individual signals are weak in isolation but become meaningful when

correlated. This allows 1inch to distinguish organic user interaction from coordinated, scripted, or automated activity.

The system is not designed for deanonymization, identity inference, or account-based attribution. It does not rely on identity or registration, but the combination of the above signals with available screening data allows the construction of internal threat profiles that model execution risk across sessions and contexts without identity attribution.

By building on data already native to DeFi, Shield demonstrates how decentralized systems can progressively adopt more effective, institution-grade risk management techniques while preserving user control, privacy, and permissionless access.

6. Execution and Market Integrity

Execution security is a native property of the baseline 1inch infrastructure: atomic settlement, intent-based constraints, and MEV-resistant designs form the baseline environment in which 1inch operates.

1inch Shield is designed to operate within this environment, aligning detection, screening, and response with routing paths that are already constrained by design.

6.1. Protection by Design

At the core of the 1inch ecosystem, execution is deterministic, atomic, and tightly bound to user intent.

In swap aggregation mode, transactions are executed atomically through immutable smart contracts. All transaction parameters are fixed at signing, and any attempt to modify them or alter execution flow causes the transaction to revert on-chain.

To make these guarantees meaningful in practice, 1inch applies pre-execution validation during transaction construction to prevent browser-level overrides, injected routing parameters, or manipulated UI inputs from influencing what the user ultimately authorizes. The transaction either completes exactly as authorized or does not occur at all. Before call data is generated and presented for signing, relevant risk checks are performed on the initiating wallet, the assets involved, and the proposed execution path. Calldata is constructed and surfaced for signing only once these checks pass.

Intent-based swaps, including cross-chain, extend this protection further. Users sign structured intents defining acceptable outcomes (price bounds and asset constraints). Execution rights are resolved through an auction mechanism:

- only the resolver selected through auction may execute the intent, and
- execution must occur using the wallet that signed the original intent.

This architecture enforces execution exclusivity, prevents calldata manipulation, and materially reduces front-running opportunities.

6.2. Market Manipulation Controls

Execution correctness alone does not guarantee market integrity. Certain forms of abuse exploit coordination gaps between transactions, liquidity, and timing, producing outcomes that are technically valid yet economically harmful.

To address this, the framework considers market-level behavioral signals that may indicate:

- front-running and sandwich attacks,
- abnormal routing behavior indicative of manipulation, and
- coordinated activity that exploits latency or visibility asymmetries.

User-facing protections complement detection at the call data construction level. Interface- and browser-level spoofing defenses help prevent deceptive presentation of prices, routes, or transaction outcomes – attacks that target user perception rather than protocol logic.

6.3. Structural MEV Mitigation

Some adversarial strategies cannot be reliably mitigated through monitoring alone. For these cases, 1inch relies on execution designs that reduce extractable value by construction.

1inch RabbitHole in swap aggregation is a decentralized execution mechanism designed to prevent back-running and other toxic MEV strategies.[9] By altering execution ordering and settlement mechanics, RabbitHole removes the economic incentives that make these strategies viable in the first place.

As described before, 1inch **intent-based infrastructure** advances this approach by separating user intent from execution path construction. Deterministic matching, resolver exclusivity, and cryptographic enforcement of execution constraints limit the ability of third parties to insert themselves into transaction flows.

[9] 1inch (2022), *The 1inch RabbitHole: protection from sandwich attacks*, 25 Nov 2022, 1inch Blog, https://blog.1inch.com/the-1inch-rabbithole-protection-from-sandwich-attacks/

6.4. Emerging Market-Integrity Research (Forward-Looking)

As DeFi matures, some of the most damaging risks no longer arise from individual transactions but from coordinated market behavior over time. Rug pulls, deceptive liquidity exits, and exploit-driven liquidity migration often unfold across multiple blocks, venues, and wallets, appearing benign when viewed one transaction at a time, yet clearly harmful in aggregate.

To better understand these risks, 1inch is exploring analytical approaches that may help surface complex market patterns earlier than conventional monitoring techniques. These approaches remain exploratory and may evolve as the ecosystem develops new analytical methods. Examples of patterns that may be studied in this context include:

- liquidity concentration followed by asymmetric withdrawals
- coordinated liquidity exits that disadvantage other participants
- artificial or spoofed trading activity designed to distort demand signals
- coordinated movement of funds across addresses and venues that may indicate planned extraction rather than organic market activity

For example, academic and industry research has explored the use of machine-learning techniques to identify potential risk signals in newly deployed token contracts based on early liquidity behavior and structural features. Such approaches illustrate how analytical tools may help surface early warning indicators, though these methods remain an evolving area of research.

Intent-based execution models may also create opportunities for future analytical improvements. Because user intent is

separated from execution path construction, this architecture may enable analytical tools that evaluate market conditions or asset characteristics before determining how execution occurs.

For example, future analytical approaches could potentially evaluate how particular token pairs behave under different execution mechanisms and adapt routing strategies accordingly. In certain circumstances, auction-based execution may improve outcomes, while in others automated market maker execution may remain the more efficient path.

Such approaches remain exploratory and would be designed to reduce exposure to potential manipulation strategies or unnecessary execution surface area, particularly for assets that lack reliable price references.

Importantly, these approaches are complementary and forward-looking. Their purpose is to explore how decentralized infrastructure may eventually gain earlier, probabilistic visibility into systemic market risks.

These concepts illustrate potential directions for market-integrity research within decentralized infrastructure and should not be interpreted as a description of currently deployed monitoring systems.

7. Incident Detection, Investigation, and Coordinated Response

In decentralized infrastructure, incidents are not exceptional events. Exploits, phishing campaigns, and coordinated abuse are a persistent reality, often propagating across protocols and venues faster than any single actor can react in isolation. Resilience, therefore, is not achieved through unilateral control, but through early detection, disciplined investigation, and real-time coordination across the ecosystem.

7.1. Proactive Monitoring and Investigation

1inch's incident posture begins with continuous, proactive monitoring.

Key sources include:

- 1inch Shield-native monitoring, as described throughout this paper.
- Zero-day exploit intelligence, including real-time incident feeds from partners such as ZeroShadow, which specialize in surfacing emergent attack vectors and active exploit indicators as incidents unfold.
- Ecosystem and community reporting, such as disclosures from independent investigators, security teams, and public watchdog initiatives, which are triaged, validated, and correlated before operational use.
- Public integrity lists and issuer disclosures, including restricted address sets published by major ecosystem actors, incorporated as one signal category within a broader screening and escalation framework rather than treated as authoritative on their own.

These inputs are treated as signals, not verdicts. When monitoring thresholds are crossed, incidents may be escalated to an internal blockchain investigation function, responsible for converting raw signals into validated, actionable intelligence.

In practice, this work includes:

- Triage and validation, separating benign anomalies from credible incidents requiring response.
- Forensic reconstruction of transaction flows, ordering, and fund movement across wallets, bridges, and venues.
- Pattern correlation, linking observed behavior to known exploit templates, historical incidents, and shared threat intelligence.
- Contextual analysis, assessing how the activity interacts with transaction paths and modes and market conditions.
- Maintaining structured records of security decisions, escalation actions, and supporting intelligence to support internal review, incident analysis, and audit processes.

The output of this process is not enforcement, but clarity: what is happening, how confident the assessment is, which surfaces are affected, and what escalation path applies.

7.2. Coordinated Response: Partners and Industry Coalitions

In decentralized infrastructure, response is rarely a solo act. Incidents routinely span multiple protocols, wallets, liquidity venues, and service providers. For this reason, 1inch operates with the assumption that effective incident response must be networked by default, extending beyond any single system or control plane.

(a) Incident-response partners and war rooms

During active events, 1inch participates in rapid coordination processes focused on shared situational awareness, indicator exchange, containment strategies, and post-incident analysis. Partners such as ZeroShadow and InnerWorks support real-time incident response and composable threat-intelligence distribution, enabling faster identification of exploit flows and earlier containment across affected infrastructure.[10]

(b) Response at ecosystem scale

1inch participates in active industry coalitions focused on real-time signal sharing, containment coordination, and recovery workflows during high-impact events.

A key example is the incident-response coalition convened around ZeroShadow, which emerged following North Korea–linked thefts involving rapid, cross-ecosystem laundering.[11] This coalition brings together protocol teams, wallets, exchanges, forensic investigators, and response providers to address a core failure mode in DeFi security: fragmented response to coordinated attacks.

Within this framework, participants collaborate to:

- exchange exploit indicators and laundering heuristics in real time,
- align containment and voluntary response actions where legal enforcement lags,
- coordinate recovery-oriented workflows and victim support,
- and reduce duplication by sharing validated intelligence across the ecosystem.

---

[10] 1inch (2025), *How 1inch security investigation flow works*, 27 Nov 2025, 1inch Blog, https://blog.1inch.com/1inch-security-investigation-flow/

[11] zeroShadow (2025), *North Korea Laundered $1 Billion of Crypto in 4 Months. How Industry Leaders Can Change Crypto Freezes and Recovery,* zeroShadow Blog, 16 Jul 2025, https://www.zeroshadow.io/blog/north-korea-laundered-usd1-billion-of-crypto-in-4-months-how-industry-leaders-can-change-crypto/

Complementary coordination channels include:

(a) SEAL 911 escalation paths

SEAL 911 functions as a 24/7 emergency response channel connecting affected projects with trusted responders during ongoing or imminent incidents.[12] 1inch's escalation framework is designed to interoperate with such emergency pathways when time-critical coordination is required.

(b) Crypto ISAC information sharing

Crypto ISAC facilitates structured sharing of indicators of compromise, adversary techniques, and emerging threat patterns across participating members. Engagement in these forums reduces duplicated investigation effort and materially shortens ecosystem-wide response timelines.

1inch operates on the assumption that real incidents require real-time coordination across protocols, wallets, investigators, and responders, not isolated action by any single system.

7.3. Real-World Response

Where incidents intersect with criminal activity, sanctions exposure, or broader public interest concerns, 1inch cooperates, where legally appropriate, with relevant authorities.

This cooperation typically involves:

- sharing validated technical context (execution traces, behavioral patterns, incident timelines),
- responding to lawful information requests, and
- using inbound intelligence as another input into Shield's screening and escalation processes.

Hence, the 1inch non-custodial system becomes institution-grade in practice: not by asserting control, but by demonstrating operational readiness: fast detection, disciplined triage, and credible coordination when it matters.

8. Enterprise-Grade Controls Supporting Shield

While 1inch Shield defines how risk is identified and addressed in decentralised systems, operating such controls at scale requires additional enterprise-grade controls. These controls operationalize 1inch Shield, translating real-time security signals into disciplined governance, integrity, and accountability, without compromising non-custodial execution, user control, or privacy.

This section describes the supporting controls that enable Shield to function responsibly in a production environment serving both retail and institutional users.

8.1. Financial Integrity Without Custody (Sequestration)

Sequestration exists to preserve financial integrity, not to enforce user behavior. It applies exclusively to infrastructure-owned revenue (surplus, fees) and operates independently of user funds or execution, which remain fully non-custodial.

Isolation mechanism. Where internal analysis or external intelligence indicates that infrastructure revenue may be linked to illicit

[12] See *Security Alliance (SEAL):* https://securityalliance.org/our-work/seal-911

activity or exploit propagation, the associated amounts are segregated into designated isolation wallets. These wallets are fully separated from operational funds and are incapable of generating economic benefit during the review period.

Governance and auditability. All sequestration actions are governed by predefined internal policies. Events are logged, reviewable, and auditable, with clear attribution of decision authority and rationale. Sequestration is not an enforcement tool against users; it is an internal risk-hygiene measure applied to infrastructure revenue only.

Sequestration demonstrates how traditional financial-integrity controls can be adapted to decentralized infrastructure. It preserves auditability, supports investigations, and protects the integrity of infrastructure operations — without asserting control over user assets or execution.

8.2. Partner Verification

Integration partners, liquidity providers, resolvers, ecosystem contributors interact with 1inch infrastructure at a scale or depth that warrants additional assurance. For these relationships, 1inch applies structured verification and security review processes designed to assess operational maturity of the partner engaging on a structural level. This includes:

- formal risk classification and escalation paths,
- defined decision authority for security-related actions,
- periodic reviews aligned with infrastructure evolution, and
- documentation practices that support traceability and audit readiness.

8.3. Risk Governance

Shield operates within a broader enterprise-grade risk governance framework that defines how security signals are interpreted, escalated, and acted upon across the organization.

At its core, this framework establishes:

- formal risk classification and prioritization standards,
- predefined escalation paths tied to severity, scope, and potential impact,
- clearly assigned decision authority for security-related actions, and
- documentation practices that preserve context, rationale, and auditability.

Enterprise governance also extends beyond purely technical threats. Social engineering, insider risk, and operational misuse are addressed through organizational controls, including role-based access restrictions, segregation of duties, recruitment-level safeguards for security-sensitive roles, and internal procedures for reporting and review.

These governance practices are reinforced by enterprise-grade risk management standards, including certification under the ISO/IEC 27001 and SOC 2 (Type 1) frameworks, which provide a structured framework for information security governance, risk assessment, and continuous improvement across infrastructure and operations.[13]

[13] 1inch (2025), *ISO27001 certification reinforces 1inch's security-first approach*, 30 Oct 2025, 1inch Blog, https://blog.1inch.com/iso27001-certification/

9. Education and Transparency

The risk management framework does not end at detection and enforcement. In decentralized systems, informed users are part of the security surface.

Educational Content and the 1inch Academy (Evolving). Today, risk and security education at 1inch is delivered primarily through public-facing content, including blog posts, guides, and incident explainers. This material covers:

- scam awareness, phishing prevention, and common attack patterns,
- explanations of security-relevant product features such as MEV protection, intent-based orders, and transaction simulation, and
- practical guidance on self-custody risks, wallet access, recovery, and the use of smart account features available in the ecosystem.

This body of content is being progressively structured into the 1inch Academy – a dedicated educational hub intended to organize these resources into clearer learning paths and reference materials.

Public Security Disclosures. 1inch regularly publishes security-related updates, including incident analyses, audit summaries, and information on threat-intelligence partnerships. These disclosures are intended to share lessons learned, surface emerging risks, and contribute back to the ecosystem.

Demonstrable Controls (Upcoming). To complement education and disclosure, 1inch is developing a demonstrable controls page that will surface aggregate, real-time indicators such as:

- the number of wallets blocked at interface or protocol layers,
- active risk alerts and escalations, and
- token-level warnings currently in effect.

The objective is visibility without voyeurism: showing that security systems are active and responsive, without exposing individual users or sensitive operational details. In the interim, these metrics are monitored internally through dedicated analytics dashboards to track effectiveness, trends, and operational performance of Shield controls.

Together, education, disclosure, and demonstrable signals close the loop ensuring that risk management at 1inch is not only enforced, but understandable and verifiable.

10. Extending 1inch Shield

1inch Shield is intended to be an adaptable and integratable infrastructure rather than a closed, internal system.

While it is tightly integrated into 1inch's own stack, its underlying principles: integral risk assessment, multi-surface screening, and non-custodial governance, are intentionally portable.

DeFi Back-Office Tooling. 1inch is developing back-office capabilities intended for DAOs, protocols, and institutional DeFi operators. These tools focus on operational security rather than custody and include:

- dashboards for transaction monitoring and oversight,
- wallet vetting and counterparty screening, and
- audit-ready reporting designed to support internal governance and external review.

The objective is to bring familiar operational discipline to DeFi environments without introducing centralized control over assets or transactions.

Shield principles and tooling are being evaluated for integration into partner environments, including institutional and DAO-operated systems, serving both institutional adoption and DeFi native communities.

Conclusion

Decentralized finance has already crossed the threshold into shared financial infrastructure. The question now is not whether non-custodial decentralised systems work, but whether they can remain reliable, resilient, and intelligible as complexity increases. As decentralised systems coordinate liquidity across chains, protocols, and execution models, the primary differentiator becomes how well they manage risk that emerges at all layers and stages of transaction.

The architecture described in this paper reflects a view of risk management as an integrated property, not an external constraint. By embedding risk awareness into all layers of a protocol or application, correlating signals across actors and interaction surfaces, and supporting these mechanisms with disciplined governance, investigations, and ecosystem coordination, 1inch demonstrates how decentralized systems can scale without reverting to custody, identity, or discretionary control. This approach does not dilute DeFi's core principles—it operationalizes them. As decentralized infrastructure expands to support more sophisticated markets and tokenized real-world assets, native risk framework is no longer a differentiator. It is the minimum bar for credibility at scale.