Defense-in-Depth Readiness Assessment for Digital Asset Operations

Use this assessment to evaluate whether your security architecture can withstand modern digital asset threats.

This is not a compliance checklist. It is designed to test whether your controls could remain effective under realistic failure conditions, including compromised endpoints, stolen credentials, malicious insiders, and manipulated transaction interfaces.

Answer each question using an assume-breach mindset: if a single user device, admin account, cloud environment, or integration were compromised, would independent controls still prevent unauthorized fund movement? “Yes” should mean the control is enforced by architecture and cryptography, not dependent on procedure, trust, or manual review.

Any uncertainty is a signal to investigate, as attacks in digital assets typically exploit the gaps between people, process, and technology.

Transaction Intent & Initiation Controls

Protect against phishing, UI manipulation, API compromise

□ Does your system require independent verification for transactions, even if a workstation, browser, or CI/CD pipeline is compromised?

□ Are transaction initiation channels (UI, API, integrations) cryptographically authenticated to a trusted execution environment?

□ Are API credentials:

- Least-privileged by default?
- Bound to IP ranges and environment context?
- Unable to trigger withdrawals without additional independent approval?

□ Does your system prevent display manipulation attacks that show operators different data than what is signed?

If transaction intent can be altered upstream of signing without independent verification, you are exposed to Bybit-style attacks.

Transaction Approval & Human Verification

Protect against blind signing, social engineering, insider coercion

□ Do approvers view transaction details on independent, hardware-secured devices?

□ Are approval devices isolated from:

- ▲ The initiating workstation?
- ▲ Corporate endpoint management systems?

□ Is the transaction data:

- ▲ Decoded into human-readable actions?
- ▲ Simulated against the current blockchain state?

□ Are unlimited approvals, hidden token transfers, and signature requests that grant unintended spending rights flagged before signing?

If approvers rely on a single UI or sign opaque payloads, this creates a blind-signing risk, even with multi-sig.

Private Key and Wallet Architecture

Protect against private key compromise, insider access, infrastructure attacks

□ Are private keys prevented from ever existing in full at any point, including generation, storage, signing, and backup?

□ Are key shares:

- ▲ Distributed across independent fault domains?
- ▲ Protected inside hardware-isolated secure enclaves?

□ Are cloud administrators, DevOps staff, and SREs prevented from:

- ▲ Accessing key material?
- ▲ Influencing signing logic?

□ Can key shares be rotated or refreshed without changing wallet addresses?

If any individual, machine, or cloud environment can reconstruct keys, you have a structural single point of failure.

Policy, Governance, and Change Management

Protect against insider threat, collusion, privilege abuse

□ Are transaction policies:

- ▲ Cryptographically enforced?
- ▲ Protected from unilateral admin modification?

□ Do policy changes require:

- ▲ Multi-party admin quorum?
- ▲ Independent device approval?

□ Is there a complete, immutable audit trail for:

- ▲ Policy changes?
- ▲ Approval overrides?
- ▲ Admin actions?

□ Are administrators prevented from unilaterally reducing approval thresholds or whitelisting destinations?

Insider risk is not solved by trust. It is solved by enforced separation of authority.

Onchain Interaction and DeFi Risk Controls

Protect against wallet drainers, malicious contracts, and address poisoning

□ Are smart contract interactions restricted to pre-approved, reviewed contracts?

□ Can transactions be simulated and decoded before approval, not only after execution?

□ Are high-risk patterns explicitly flagged, including unlimited token approvals and signature requests that grant unintended spending rights?

□ Are all deposit addresses exchanged through authenticated channels, eliminating manual copy-paste?

□ Are address poisoning and clipboard malware attacks prevented from routing funds to attacker-controlled wallets?

Allowing users to interact freely with arbitrary contracts or addresses keeps DaaS and address-poisoning viable.

Resilience, Detection, Blast-Radius Control

Protects against major damage if breach occurs

- □ If one security layer fails (endpoint, admin account, cloud region), do additional independent controls prevent unauthorized fund movement?
- □ Can you:
  - ▲ Detect anomalous behavior in real time?
  - ▲ Attribute actions to specific identities and devices?
- □ Are signing components geographically and operationally isolated?
- □ Can operations continue if a subset of infrastructure is disabled or compromised?

Resilience matters as much as prevention when attackers are persistent and well-resourced.

Organizational Readiness and Accountability

Aligns people and process with technology

- □ Are roles clearly separated between:
  - ▲ Initiators?
  - ▲ Approvers?
  - ▲ Policy administrators?
  - ▲ Infrastructure operators?
- □ Are high-risk actions:
  - ▲ Rare by design?
  - ▲ Observable by default?
- □ Do incident response plans explicitly cover onchain theft scenarios, not just IT breaches?

Security technology requires organizational discipline and accountability to be most effective.

If these questions reveal any uncertainty, ambiguity, or reliance on trust rather than enforced controls, your organization could be exposed to the same failure modes used in recent billion-dollar attacks.

Fireblocks' defense-in-depth architecture is designed to address these gaps—not through point solutions, but through layered, cryptographically-enforced controls.

This architecture is trusted in production by over 2,400 enterprises, has secured more than $10 trillion in digital asset transactions, and protects over 550 million wallets globally.

To learn more about protecting your digital assets, reach out to info@fireblocks.com, or visit Fireblocks.com.