Fireblocks®

Cheat Sheet: The Four Pillars for Building Operational Security in Digital Assets

Building your team with trust

- ☑ Examining your people – validate references, work experience, and backgrounds.
- ☑ “Limit the blast radius” – establish basic role-based permissions that manage access controls from financial and operational tasks to smart contract deployments.
- ☑ Use multi-factor authentication or hybrid security keys for anything not on-chain.
- ☑ Establish or hire a main security point of contact - the security expert on your team.

AICPA SOC 2 · ISO 27001 · ISO 27017 · ISO 27018 · CCSS Qualified Service Provider

System Design: map and monitor all external infrastructure dependencies

- ☑ Utilize key management systems provided by vendors that have in-depth expertise, have been audited and are battle-tested – there are too many threat vectors and too much niche expertise needed to build these capabilities internally at a speed that allows you to keep up with the market while remaining secure.
- ☑ Analyze and map the dependencies and vulnerabilities for external infrastructure systems such as external services, smart contracts, or oracles.

Continuous Improvement: build with security in-mind

When launching an MVP

- ☑ Test yourself and your code (there are many good solutions on the market today that can help with this).
- ☑ Define your key invariants, for modules and methods, and document it for yourself (this will also help make working with auditors more efficient and effective).

Staying secure in production

- ☑ Create a bug bounty program or partner with someone that can offer it to you.
- ☑ Ensure you have good operational security for CI / CD.
- ☑ Manage patch-gapping for open-source software (fix it on your side first before pushing anything new to GitHub).
- ☑ Test and document your invariants for every code commit and release to ensure you are not breaking your key assumptions.

Red Teaming and Incident Preparedness

Think like a hacker and test your systems

- ☑ Identify gaps and ways your system can be hacked and document it.
- ☑ Create an appropriate plan to deal with these issues should they arise.