TGE security readiness checklist

Architecture

□ Architecture documentation review completed by external experts

□ (economic and technical)

□ Technical documentation updated to match the shipping codebase

Threat model created and risk mitigation in place

Operational

□ Safety operations: reporting, configuration workflows, enforcement policy

Upgrade and admin pathways documented (who can change what, and how).

□ Emergency controls implemented and tested.

□ All technical and non-technical staff are informed about attack vectors and have operational security knowledge.

□ Multisig Operations policy defined.

□ Incident response plan finalized (roles, escalation, communications, “stop conditions”, external experts for war room staffing)

□ System monitoring in place, ideally one dashboard for alerts for anomalies

- ○ Backend/Frontend/Servers/third-party APIs
- ○ Markets: Oracle issues, liquidity events
- ○ Smart contracts and contract interactions

□ Internal security review completed (keys, access, dependencies, monitoring).

Team Management / Day-to-Operational Practices

□ Team KYC / Background checks completed

□ Secure Communication Guidelines

□ Authentication checks and enforcement tested

□ Phishing resistance guidelines

□ Device Management policies

□ Provider security review (DNS provider and setup, hosting, tooling)

Testing

□ Internal code review

□ Test case coverage as high as possible, informed by the threat model

□ If applicable, fuzz testing and formal verification are defined and executed

□ Core protocol contracts deployed and verified (production configuration)

External validation and reinforcement of security

□ Independent audit(s) completed; findings remediated and verified, threat model updated.

□ Penetration testing of web2 infrastructure completed

□ Bug bounty policy defined and published

□ Optional: Physical security training for key team members

OAK