Area	Generic Web3 Risk Profile	ICP-specific Differences / Additional Risks
Key custody	HSM/MPC/multisig recommended for private keys & signers	Same plus replica DKG material, neuron keys, Internet Identity anchors; controller principal management unique
Upgrade paths	Upgradeable contracts, proxies, timelocks	Canister upgrades, controller principals, staged upgrade/ migration concerns; NNS governance auto-upgrades
Node/operator risk	Validator collusion, equivocation, censorship	Replica operators and DKG/key exposures; boundary node operator risks and HTTP gateways
Oracles & Bridges	Multi-source oracle, relayer risks, cross-chain proofs	Adapters/bridges to non-ICP chains, off-chain adapters used by ICP; oracle medianization still relevant
MEV/mempool	MEV, front-running, transaction privacy issues	Mempool exposure varies by protocol; ICP-specific ingress patterns reduce classical mempool MEV but front-run-like risks remain at ingress/relay layers
Supply chain	CI/CD artifacts, malicious packages	Same plus DFX/sdk-specific toolchain, WASM artifact provenance and deterministic builds
Governance	DAO capture, flash-proposal	NNS neuron governance, proposal auto-execution risks, neuron compromise
Observability	On-chain monitoring, watchlists	Need for replica/canister state diffs, boundary node telemetry, Internet Identity event tracking