CAPITAL MARKETS RISK MITIGATION FRAMEWORK (RMF)

RISK ASSESSMENT PARTNER: CLPR (CROSS-LEDGER PROTOCOL)

clpr

WHAT IS THE RMF?

The Capital Markets RMF is an industry-led framework designed to help financial institutions identify, assess, and manage the non-financial risks associated with using public permissionless blockchain infrastructure

WHAT ARE RAPs?

RMF's Risk Assessment Partners (RAPs) are the industry leaders and solution builders who have committed to proof-testing the RMF through real-world pilots

ABOUT CLPR

CLPR (Cross-Ledger Protocol, pronounced "clipper") is a bridgeless cross-ledger messaging protocol in development by Hashgraph and contributed to Linux Foundation Decentralized Trust (LFDT) as an open source Lab. CLPR uses cryptographic state proofs to allow independent blockchain networks to verify each other's state directly, with no bridge operator, no pooled collateral, and no intermediary in between

HOW IT WORKS

01 Send
An application hands its message to CLPR on Chain A, where it is approved, numbered and queued.

02 Prove
Chain A's validators jointly sign a record that includes it. An endpoint fetches that signed proof.

03 Verify and deliver
Chain B checks the proof against Chain A's own signature, then runs the receiving application.

04 Reply comes home
Every accepted message gets exactly one reply, proved back to Chain A the same way.

ALIGNMENT WITH THE RMF

RMF Risk Area	How CLPR Addresses It
Third-Party and Counterparty Dependency Risk	CLPR helps eliminate the bridge operator entirely. Trust runs ledger-to-ledger, enforced by cryptographic state proofs. No third party holds custody of assets at any point in a CLPR-based transfer
Custody and Asset Safety Risk	CLPR-enabled applications that use a burn-and-mint pattern require no pooled collateral. This path requires asset issuers to opt in, deploying an adapter contract and granting mint/burn rights on their token. Where an issuer has done so, assets are burned on the source chain and minted natively on the destination, with nothing held in custody at the protocol layer
Operational Resilience and Single Points of Failure	CLPR is designed with no single point of failure at the protocol level. If relay endpoints go offline, transfers pause and resume automatically, so funds are never at risk
Smart Contract and Verifier Risk	Hashgraph treats verifier contracts as the highest-priority security-critical code in the CLPR system. Any change requires heightened review; CI is configured to fail on any finding against CLPR smart contracts
Governance and Protocol Dependency Risk	CLPR has been contributed to Linux Foundation Decentralized Trust (LFDT) as an open source lab, with the codebase publicly available on GitHub. This removes single-entity control of the protocol's direction and gives regulated institutions a structured path to participate in shaping it

ACCESS RMF: RMF.GBBC.IO // LEARN MORE: HASHGRAPH.COM/CLPR