LINKMERICA

Institutional Custody Risk Intelligence

LISR Advisory Report

Meridian Family Office (illustrative)

Report Reference	LM-ADV-SAMPLE-001
Client ID	SAMPLE
Client Type	Single-Family Office — Sample Engagement
Report Date	2026-07-31
Framework	LISR-v1.0
Prepared by	The Linkmerica Research Team
Classification	SAMPLE — PUBLIC · NOT A CLIENT REPORT

SAMPLE — ILLUSTRATIVE ONLY

SAMPLE — ILLUSTRATIVE ONLY. The client, portfolio and circumstances described in this report are fictional and were constructed to demonstrate report structure. The LISR scores, category breakdowns and risk flags are NOT fictional: they are the actual published Linkmerica ratings as of the report date, and can be verified against linkmerica.com and the public integrity hash log. No real client engagement is represented. Redacted fields in a live report would include entity name, holdings, addresses and key-holder identities.

01

Executive Summary

This sample LISR Advisory Report assesses two hardware wallet families under consideration for a two-of-three multisignature custody arrangement with an inheritance provision. Ledger scores 4.8 (MODERATE). Trezor scores 4.7 (MODERATE). Neither device family scores in the LOW tier, and the LISR scale is inverted — a higher score indicates higher custody risk. The two devices score within 0.1 of one another but for materially different reasons: Ledger's risk concentrates in closed-source firmware and centralised supply chain, Trezor's in the architecture of its pre-Safe-series devices. A multisignature arrangement combining both manufacturers is therefore assessed as reducing correlated vendor risk relative to a single-manufacturer deployment. The engagement profile includes no agentic payment exposure; the ACR dimension is not applied.

SCORE SUMMARY

Wallet	Composite Score	Risk Tier	LISR Version
Ledger	4.8 / 10.0	**MODERATE**	LISR-v1.0
Trezor (pre-Safe-series)	4.7 / 10.0	**MODERATE**	LISR-v1.0

Scope note

The Trezor assessment reflects pre-Safe-series devices (Trezor One and Model T generation). Trezor Safe 7 carries a separately published Quantum Resistance Readiness score and is not covered by this LISR assessment. Device generation materially affects findings — see linkmerica.com/corrections/ for the dated record of this distinction.

02

LISR Methodology Overview

The Linkmerica Institutional Security Rating (LISR) framework is a deterministic, version-controlled scoring system for institutional-grade custody risk assessment. All scores are locked at version publish and cannot be retroactively altered.

SCORING CATEGORIES

Security Architecture

Cryptographic design, secure element implementation, physical attack resistance.

Firmware Integrity

Firmware signing, update verification, reproducible build status, vulnerability disclosure.

Supply Chain Risk

Manufacturing provenance, anti-tamper mechanisms, distribution chain controls.

Key Management

Seed generation, entropy quality, BIP-39 implementation, passphrase support.

Operational Security

PIN lockout controls, duress mechanisms, air-gap quality, display verification.

Recovery Risk

Seed backup mechanisms, metal backup compatibility, recovery phrase standardisation.

SCORING SCALE

Score Range	Risk Tier	Interpretation
0.0 – 3.5	LOW	Suitable for institutional consideration with standard diligence
3.6 – 6.0	MODERATE	Requires additional controls or policy mitigations
6.1 – 8.0	HIGH	Significant risk factors — limited institutional suitability
8.1 – 10.0	CRITICAL	Not recommended for institutional custody use

03

Wallet Assessment: Ledger

4.8 / 10.0	MODERATE RISK	LISR-v1.0
COMPOSITE SCORE	RISK TIER	FRAMEWORK VERSION

CATEGORY BREAKDOWN

Security Architecture 3.2

3.2

Certified secure elements (CC EAL5+), ST31/ST33 chips.

Firmware Integrity 6.4

6.4

Cryptographically signed but closed-source; no reproducible build verification.

Supply Chain Risk 6.2

6.2

End-to-end manufacturing and distribution centralised under one vendor.

Key Management 2.8

2.8

Secure element hardware RNG, NIST SP 800-90A/B compliant. Passphrase supported.

Operational Security 3.4

3.4

PIN enforced by secure element with escalating lockout.

Recovery Risk 4.2

4.2

BIP-39 compliant; cross-device restoration reduces vendor lock-in.

ANALYST NOTES

Strongest of the assessed pair on security architecture (3.2) and key management (2.8), anchored by CC EAL5+ certified secure elements. Risk concentrates in firmware integrity (6.4) and supply chain (6.2): firmware is cryptographically signed but closed-source, preventing reproducible-build verification, and manufacturing and distribution are centralised under a single vendor.

04

Wallet Assessment: Trezor (pre-Safe-series)

4.7 / 10.0	MODERATE RISK	LISR-v1.0
COMPOSITE SCORE	RISK TIER	FRAMEWORK VERSION

CATEGORY BREAKDOWN

Security Architecture 5.5

5.5

Varies by product line; Trezor One lacks a secure element.

Firmware Integrity 2.8

2.8

Fully open-source firmware; independently verifiable.

Supply Chain Risk 6.2

6.2

Third-party contract manufacturing, primarily Czech Republic.

Key Management 3.2

3.2

BIP-39 with on-device entropy from hardware RNG plus host entropy.

Operational Security 4.5

4.5

PIN with exponential backoff on failed attempts.

Recovery Risk 3.8

3.8

Standard BIP-39 12 or 24-word mnemonic displayed on-device.

ANALYST NOTES

Strongest of the assessed pair on firmware integrity (2.8) — fully open-source and independently verifiable, the inverse of Ledger's profile. Risk concentrates in security architecture (5.5), driven by the absence of a secure element in Trezor One and documented physical side-channel exposure, and in supply chain (6.2). Assessment covers pre-Safe-series devices only.

05

Recommendations

01 Distribute the two-of-three quorum across both manufacturers rather than three devices from one vendor. The two families fail differently; correlated failure is the risk a single-vendor quorum does not address.

02 Treat Ledger's closed-source firmware (6.4) as an audit limitation to be documented in custody policy, not as a disqualifier. It cannot be independently verified; that fact should be recorded rather than assumed away.

03 For any Trezor device in the quorum, confirm the specific model. The pre-Safe-series findings in this report do not transfer to Safe 7, which has a materially different security architecture.

04 Establish and document the inheritance recovery procedure before deployment. Recovery risk scores 4.2 (Ledger) and 3.8 (Trezor); both rely on BIP-39, which is portable but places the entire burden on seed custody.

05 Retain this report as a versioned custody policy document. Scores are locked and hash-verifiable at the report date; later rescores do not alter this record.

06

Disclaimer & Limitations

This report has been prepared by The Linkmerica Research Team on behalf of CASPO LLC, operating under the trade name Linkmerica. It is provided for informational and risk intelligence purposes only and does not constitute investment advice, legal advice, or a recommendation to purchase, hold, or sell any asset.

The LISR framework produces deterministic risk scores based on publicly available technical specifications, disclosed firmware histories, and published security research. Scores reflect the assessed wallet's risk profile at the time of evaluation and are subject to change upon material updates to device firmware, supply chain structure, or security posture.

This report is a published SAMPLE describing a fictional client. It carries no confidentiality classification. The LISR scores it cites are the actual published Linkmerica ratings as of the report date, verifiable against linkmerica.com. Redistribution without written consent of CASPO LLC is prohibited. CASPO LLC is a Virginia limited liability company. Linkmerica is a trade name of CASPO LLC, filed with the Virginia State Corporation Commission.

Report Reference: LM-ADV-SAMPLE-001 · Report Date: 2026-07-31 · Prepared by: The Linkmerica Research Team ·