MERIDION
RISK

METHODOLOGY

How Meridion Risk evaluates digital assets

Every Meridion report separates two questions: what can go wrong, and how strong is the evidence? Risk and confidence are rated separately so readers can distinguish a weak asset from a weak evidence base.

Three domains

Each assessment starts with three standalone judgments. Clean code does not erase weak operations. Strong reserves do not excuse brittle upgrade control. Each domain receives its own risk rating before we derive an asset-level conclusion.

DOMAIN I

Smart Contract Security

We look for exploitable code paths, unsafe upgrade mechanics, hidden runtime surface, and weaknesses that could directly affect balances, supply, transferability, or contract control.

DOMAIN II

Operational Security

We map who can act, how quickly they can act, and what stands between a privileged function and an irreversible mistake, key compromise, governance capture event, or emergency failure.

DOMAIN III

Financial Integrity

We assess backing quality, reserve visibility, liquidity under stress, redemption design, legal structure, regulatory exposure, and counterparties that could determine whether holders can exit.

Risk ratings

Domain ratings use three labels: Low, Medium, and High. Low means no material adverse condition was found inside the assessed scope. Medium means there is a real weakness or dependency, but it is buffered, contingent, or not currently causing holder harm. High means there is a credible path to direct holder harm, loss of control, impaired transferability, severe depeg, asset shortfall, or material financial stress.

COMPOSITE RATING	MEANING
Minimal	All three domains are Low, with no material identified weakness beyond ordinary residual risk for that asset type.
Low	No domain is High, and any Medium condition is isolated, buffered, or not immediately consequential for holders.
Moderate	The asset has meaningful risk but no active high-severity failure mode. This usually means multiple Medium domains, or one structurally important Medium condition.
Elevated	At least one domain is High, but the issue remains contingent and is not yet causing active holder harm.
High	A direct holder-facing consequence is present, or a High condition bears on holders in an immediate way.
Severe	Multiple domains are breaking at once, or one failure mode can cascade through the full asset structure.

Confidence ratings

Confidence is not averaged into risk. A rating describes the risk we found. Confidence describes how complete, current, independent, and reproducible the evidence is. A Low-risk, Low-confidence result is not equivalent to a Low-risk, High-confidence result: it means the available evidence did not prove a material problem, but important facts remain less certain.

MORE CONFIDENCE

What raises confidence

Primary evidence, reproducible on-chain checks, verified bytecode and source, independently maintained datasets, current reserve assurance, and a scope that captures the important contracts, chains, counterparties, and control paths.

LESS CONFIDENCE

What reduces confidence

Issuer-only claims, stale disclosures, off-chain controls we cannot test, excluded chains, opaque reserve components, undisclosed key management, or any material fact that would move the conclusion if it turned out differently.

Assessment process

A Meridion assessment is not a code audit with financial commentary attached. It is a combined review of code, control, and balance-sheet risk, reconciled into one asset-level judgment.

STEP 1

Map the system

Identify the in-scope contracts, chains, issuers, privileged roles, redemption paths, legal entities, and material off-chain dependencies.

STEP 2

Verify the mechanics

Use source review, bytecode checks, entry-point mapping, fork-based behavior tests, invariant review, and exploit analysis to understand what the deployed system can actually do.

STEP 3

Assess control

Examine who holds administrative power, what key-custody evidence exists, how changes are approved, what monitoring is disclosed, what recovery exists, and which actions can happen without meaningful delay.

STEP 4

Stress the financial structure

Review reserve quality, liquidity runway, counterparty concentration, redemption design, and the legal and regulatory conditions around holder exits.

Scope limits

Every material limitation is classified by effect: no rating effect, risk-rating effect, confidence effect, or both. That keeps missing evidence from disappearing into vague caveats. If a cross-chain deployment, reserve component, governance layer, or control environment is out of scope, the report states whether that gap should make the reader less certain, more concerned, or both. In each published report, these domain ratings, confidence judgments, and scope limitations appear separately before they are combined into the final rating.