Treasury Continuity Intelligence Review v2

Flagship sample deliverable

Prepared for industry-practitioner feedback.

Intended readers: founder, CFO, treasury manager, DAO treasury committee, board member.

Prepared by: Linas Preikšaitis — Independent Treasury Continuity Research.

What this review solves

Stablecoin treasury risk is not only “will USDC or USDT depeg?”

For an operating company, DAO, protocol foundation, payment team, or startup, the real question is:

Can we keep operating if a stablecoin, custodian, exchange, chain, bridge, governance process, or redemption path fails under stress?

Treasury Continuity Intelligence turns stablecoin and treasury exposure into a board-readable decision-support artifact:

• what can fail;

• what matters most;

• what evidence supports the conclusion;

• what is unknown;

• what management should verify this week;

• how ready the organization is to recover.

This is not financial advice, legal advice, tax advice, custody, asset management, trading, or transaction execution.

Section 1 — Executive Dashboard

60-second board view

Item	Result	Board meaning
Treasury Continuity Score	64 / 100	Fragile: operating model can function, but several stress points require action before scale or board sign-off.
Recovery Readiness Score	52 / 100	Weak-to-partial: recovery paths exist in principle but are not sufficiently documented or tested.
Critical Risks	3	Issues that could interrupt access, settlement, governance response, or continuity under stress.
Material Risks	5	Manageable risks that need owners, documentation, or monitoring cadence.
Largest Single Failure Point	Single stablecoin + single primary custody/redemption route	If issuer, custodian, banking, freeze, or redemption path fails, management may not have a tested fallback.
Funds with Tested Exit Path	35%	Only part of the exposure has a documented and tested route to fiat, alternate stablecoin, or alternate settlement path.
Immediate Actions	6	Practical diligence/control actions; no allocation, trading, or custody action is recommended by this report.

Treasury Continuity Score breakdown

Continuity component	Score	Status	Interpretation
Operating Cash Protection	68 / 100	Yellow	Basic runway/payment protection exists, but stress liquidity and exit documentation are incomplete.
Custody Resilience	58 / 100	Orange	Access controls exist but recovery, backup approvers, and provider escalation path are not fully tested.
Stablecoin Concentration	46 / 100	Orange	Exposure appears concentrated in one issuer or one stablecoin family without a documented stress fallback.
Chain/Bridge Continuity	62 / 100	Yellow	Operational chain dependency is understood but outage/fallback process is not fully documented.
Yield Exposure Discipline	74 / 100	Yellow-Green	Yield exposure is limited or controlled, but monitoring and withdrawal assumptions need explicit evidence.
Governance Readiness	61 / 100	Yellow	Decision authority exists, but emergency approval thresholds and escalation timing are unclear.
Recovery Readiness	52 / 100	Orange	Playbooks are incomplete; provider contacts, redemption test, and chain/custody fallback need confirmation.

Critical risks

#	Critical risk	Why it matters	Confidence	Immediate action
1	Single operational redemption path	If the only path to fiat/settlement fails, treasury may be unable to meet obligations on time.	Medium	Document and test at least one backup exit/settlement route.
2	Custody recovery path not fully tested	Key-person, provider, or approval failure can delay access during incident.	Medium	Verify admin roster, recovery process, backup approvers, and provider escalation route.
3	Governance escalation unclear under time pressure	DAO/board/founder approval lag can turn a manageable event into a treasury failure.	Medium	Define emergency authority, quorum/approval threshold, and decision window.

Largest single failure point

The largest continuity failure point is reliance on a narrow stablecoin/custody/redemption stack without a tested fallback path. The main risk is not simply “stablecoin depeg.” It is the combination of issuer, custody, chain, provider, governance, and operational dependencies failing faster than management can respond.

Immediate actions

Urgency	Action	Owner role	Evidence needed to close
24h	Confirm current stablecoin, chain, custodian, exchange, and payment-provider exposure inventory.	CFO / Treasurer / DAO treasury lead	Exposure inventory dated and approved.

Urgency	Action	Owner role	Evidence needed to close
7d	Document primary and backup exit routes for material funds.	Treasury / Operations	Tested withdrawal/redemption or written provider confirmation.
7d	Verify custody access recovery and backup approvers.	Operations / Security / Multisig owners	Admin roster, backup signer list, provider escalation contact.
7d	Define emergency governance process.	Founder / Board / DAO treasury committee	Written threshold, quorum, emergency authority, response window.
30d	Centralize provider terms and incident contacts.	Finance / Legal / Operations	Contract excerpts, support contacts, freeze/redemption terms.
30d	Establish monitoring cadence and trigger list.	Treasury owner	Monthly review checklist plus incident trigger rules.

Section 2 — Visual Heatmaps

Visual layout guidance

The board-facing heatmap should appear as a one-page table:

• title at top: “Treasury Continuity Heatmap”;

• top-right color key;

• six rows for the six core risk categories;

• one score and color per category;

• one sentence explaining board meaning;

• one immediate action per category;

• footer showing review date, data freshness, and “not financial advice / no custody / no transaction execution.”

Use color plus text labels so the page is readable in black-and-white.

Color logic

Color	Score range	Meaning
Green	80-100	Controlled / routine monitoring
Yellow	65-79	Material but manageable
Orange	40-64	Action required before scale or stress
Red	0-39	Critical continuity weakness
Grey	Unknown	Insufficient evidence; cannot assess reliably

Board-facing heatmap

Category	Score	Color	Severity explanation	Board interpretation
Stablecoin Issuer Risk	46	Orange	Material exposure appears concentrated in one issuer/stablecoin family; backup route not fully evidenced.	Treasury may face issuer, reserve, freeze, banking, or redemption stress faster than management can respond.
Custodian / Exchange Risk	58	Orange	Provider dependency exists, but recovery and escalation procedures are not fully tested.	Funds may be safe but operationally inaccessible during account, KYC, withdrawal, or provider incident.

Category	Score	Color	Severity explanation	Board interpretation
Chain / Bridge Risk	62	Yellow	Chain dependency is known, but fallback settlement route and bridge assumptions need documentation.	Treasury may be liquid in theory but delayed by chain congestion, outage, or bridge impairment.
Yield / Protocol Risk	74	Yellow-Green	Yield exposure appears limited/controlled, but withdrawal and monitoring evidence should be explicit.	Yield is not the dominant continuity risk unless liquidity/protocol assumptions are undocumented.
Governance / Escalation Risk	61	Yellow	Emergency authority, quorum, and response time are unclear.	A manageable event can become a governance failure if no one can approve action quickly.
Recovery Readiness	52	Orange	Exit, custody recovery, provider contacts, and incident playbooks are partially documented or untested.	The organization may know what it wants to do in a crisis but be unable to execute in time.

Severity calculation

Each category is scored using:

Factor	Weight
Impact if failure occurs	35%
Likelihood under plausible stress	25%
Dependency concentration	20%
Recovery/control maturity	20%

Evidence quality can cap the score:

• exposure inventory missing: category can be Grey/Unknown;

• material data missing: maximum confidence is Medium;

• confirmed single point of failure with no recovery path: maximum score is 49.

Section 3 — Methodology & Trust Framework

Source hierarchy

Tier 1 — Primary sources

Highest weight.

Examples:

• issuer disclosures;

• governance proposals;

• official documentation;

• attestations;

• financial reports;

• official protocol documents;

• official provider terms supplied by the client;

• client exposure inventory;

• verified on-chain records.

Tier 2 — Independent analysis

Used when primary sources are incomplete or when additional interpretation is needed.

Examples:

• research providers;

• analytics providers;

• reputable industry publications;

• protocol risk reports;

• incident postmortems;

• compliance/chain analytics outputs supplied by the client.

Tier 3 — Community intelligence

Used for context only unless corroborated.

Examples:

• forums;

• social discussion;

• public commentary;

• DAO discussion threads;

• credible analyst commentary.

Confidence framework

Confidence	Definition	What qualifies
High	Strong primary evidence or multiple corroborating reliable sources; low ambiguity.	Official issuer report, latest attestation, official docs, client contract, verified on-chain data, formal governance vote.
Medium	Credible evidence but partial coverage, interpretation required, or one confirming source missing.	Tier 2 provider data, official docs with gaps, recent credible research, public governance discussion not finalized.
Low	Inferred from incomplete, stale, indirect, or single-source evidence.	Community commentary, old documentation, unverified statements, incomplete customer inventory.

Rules:

• Critical risks must show confidence.

• Low-confidence critical risks are framed as urgent verification items.

• Unknowns are visible and affect the score.

Freshness framework

Freshness label	Definition	Typical threshold
Fresh	Suitable for current decision-support.	Stablecoin/liquidity/TVL data within 48h; governance status within 48h; client inventory within 5 business days; latest issuer report.
Aging	Useful but caution required.	Market/governance data 3-14 days old; client inventory older than 5 business days; official docs not recently updated.

Freshness label	Definition	Typical threshold
Stale	Not reliable for current decision without refresh/caveat.	Market/governance data older than 14 days; old inventory; superseded provider terms.

Review process

• Collection — gather only necessary exposure, provider, custody, chain, governance, and policy inputs.

• Analysis — map exposures by function and assess issuer, custody, chain, yield, governance, and recovery risks.

• Challenge process — ask what would make each conclusion wrong; check source quality, confidence, and data freshness.

• Review process — verify every material claim has a source, confidence label, freshness label, and non-advisory action.

• Final recommendation process — provide diligence/control/governance actions only.

Section 4 — Privacy & Confidentiality

Security boundary

This review does not require:

• wallet access;

• private keys;

• seed phrases;

• signing authority;

• custody;

• transaction execution;

• exchange login access;

• bank login access;

• ability to move funds;

• ability to approve transactions.

Information needed

Input	Why needed	Acceptable format
Stablecoins used	Issuer/concentration risk	Token names and approximate percentages
Chains/networks used	Chain/bridge/settlement risk	Chain list
Custodians/exchanges/wallet types	Access/provider dependency	Provider names and structure description
Approximate exposure bands	Materiality ranking	Ranges, not exact balances if preferred
Treasury/payment function	Understand operational consequence	Operating cash, payroll, grants, customer funds, collateral, settlement, yield
Governance/approval flow	Escalation readiness	Roles, quorum, signer policy, board/DAO process
Provider terms or links	Freeze/redemption/access constraints	Public docs or redacted excerpts
Known deadlines/concerns	Prioritization	Board date, launch date, audit, DAO vote, incident concern

Data minimization policy

• Collect only what is needed.

• Use ranges instead of exact balances where possible.

• Use redacted documents where full documents are unnecessary.

• Prefer public documentation when sufficient.

• Never request control credentials or custody access.

• Keep sensitive operational details out of forwardable versions unless approved.

Client-controlled disclosure

The client controls what version is shared:

• full internal version;

• board version;

• external/adviser version;

• anonymized sample version.

Anonymized review option

The review can be anonymized by replacing names, converting balances to bands, removing wallet addresses/account IDs, and retaining only risk logic, methodology, heatmap, and board conclusions.

Section 5 — Credibility Page

Prepared by

Linas Preikšaitis

Independent Treasury Continuity Research

Professional positioning

This work is based on systems thinking, engineering background, process analysis, and operational risk review.

The focus is:

• Exposure Mapping;

• Failure Mode Analysis;

• Operational Resilience Review;

• Incident Response Design;

• Stablecoin treasury continuity;

• AI-assisted research with human review.

The review treats treasury as a system of linked dependencies: issuer, reserve, redemption, custody, exchange, chain, bridge, governance, monitoring, and recovery.

AI-assisted research with human review

AI may assist collection, summarization, structuring, and drafting. Human review is used to select sources, challenge conclusions, label uncertainty, remove unsupported claims, and keep recommendations within operational

decision-support boundaries.

AI output is not treated as evidence by itself.

Boundaries

This work is not:

• financial advice;

• investment advice;

• legal advice;

• tax advice;

• accounting advice;

• asset management;

• custody;

• trading;

• transaction execution;

• a smart-contract audit;

• a regulatory opinion;

• a guarantee of asset safety.

Credibility is established through transparency: named sources, confidence labels, visible unknowns, data freshness, privacy boundaries, conflict disclosure, and correction/versioning.

Section 6 — Board-forwardable presentation check

This report is designed so that:

• a founder can forward the executive dashboard to a CFO;

• a CFO can forward the dashboard and heatmap to a board member;

• a DAO treasurer can forward the heatmap, methodology, and privacy boundary to a treasury committee;

• a skeptical practitioner can inspect methodology before trusting conclusions.

Board-forwardable rules used:

• The first page explains the problem and score in under 60 seconds.

• Technical details are translated into operational consequences.

• Recommendations are actions management can verify, not asset instructions.

• Confidence and freshness are visible.

• Privacy boundary is explicit.

• Credibility is transparent, not exaggerated.

Section 7 — What the reader should do next

If this were a live client review, management should:

• confirm the exposure inventory;

• verify the largest single failure point;

• close the six immediate actions;

• refresh stale/aging evidence;

• decide whether residual risks are accepted, reduced, or escalated.

For practitioner feedback, the key question is:

“Would this format help a real CFO, treasury manager, or DAO treasury committee make better continuity decisions?”

Closing statement

Treasury Continuity Intelligence is serious decision-support work when it is evidence-backed, confidence-labelled, privacy-preserving, and board-readable.

The goal is not to predict markets. The goal is to help management understand whether treasury operations can survive plausible stablecoin, custody, chain, governance, and recovery stress.