4) Transparency Controls

Effective date: Friday, 30 January 2026
Version: V001.005.007
Last updated: Tuesday, 10 February 2026
Issuer: FUSAUSD Financial Ltd.

Principal place of business: Wigmore Street, Marylebone, London W1U 3RY, United Kingdom

4.1 Control objectives and control standard

1. This document (the "Controls") sets out the internal control framework used to produce, approve, and publish the Transparency Package described in the Transparency Policy (the "Policy"). These Controls are designed to support accuracy, completeness, timeliness, integrity, auditability, and appropriate access restrictions.

2. The Controls apply to: (a) calculation of Circulating Supply and activity metrics; (b) collection and valuation of Reserve data; (c) reconciliation of Reserve Market Value to Token Liabilities; (d) preparation of the published package (PDF + data files + manifest); and (e) issuance of corrections and incident disclosures.

3. These Controls are written to be compatible with independent assurance engagements and controls reporting (including controls relevant to financial reporting and system controls). The Issuer maintains evidence sufficient to support walk-throughs, sampling, and re-performance by an Assurance Provider.

4. Unless a Control explicitly states otherwise, each control is performed for each monthly Transparency Package. Certain controls are also performed daily (for example, reconciliations and limit checks) and are summarized in Section 4.4.

5. Control failures are handled under Section 4.9 (exceptions and remediation) and Section 4.10 (corrections and incident disclosures). Where a control failure could affect published figures, the Issuer treats the matter as a potential Material Event under the Policy.

6. These Controls do not replace the operational mint/burn controls, AML controls, or key management controls required for Token operations generally; they reference those controls where they are dependencies for transparency reporting.

6.1 Controls framework alignment. The control objectives in this chapter are intended to cover stablecoin operational risks addressed by the American Institute of Certified Public Accountants stablecoin controls criteria (Part II), including supply authorization and completeness, reserve data completeness and valuation, reconciliation integrity, access and key management, change control, and publication integrity, as applicable to the Issuer's defined reporting boundary.

4.2 Governance, ownership, and segregation of duties

7. Control ownership is assigned to specific roles. The Issuer maintains a current organization chart, role descriptions, and a RACI matrix in Schedule 1.

8. The Issuer appoints a Transparency Owner responsible for the end-to-end reporting process, including the reporting calendar, evidence retention, package integrity, and publication. The Transparency Owner is independent of day-to-day reserve trading decision-making.

9. The Issuer appoints a Controller (or equivalent financial control owner) responsible for reserve valuation policies, reconciliation methodology, and accounting-adjacent judgments used in reporting.

10. The Issuer appoints a Treasury Operations Lead responsible for obtaining bank/custodian statements and confirmations, maintaining Reserve account registers, and supporting reconciliation with primary evidence.

11. The Issuer appoints a Blockchain Data Lead responsible for Circulating Supply calculations and chain-level activity metrics, including maintenance of in-scope contract address registries and data source validation.

12. The Issuer appoints a Security Owner responsible for the publication signing keys, access control enforcement, and security review of disclosure artifacts that could elevate theft or fraud risk.

13. The Issuer appoints a Legal/Compliance Reviewer responsible for reviewing incident notices and disclosures for compliance with applicable law, sanctions restrictions, and regulator expectations.

14. The Issuer appoints an Approver (CFO, CRO, or delegated officer) responsible for final approval of the package prior to publication, including sign-off that the backing conclusion and reconciliation are supported by evidence.

15. Segregation of duties is maintained so that no single person can: (a) move Reserve assets, (b) modify the reporting dataset or pipeline, (c) approve the package, and (d) publish the package. At least two individuals are required for package publication: one to prepare and one to approve.

16. Access rights are reviewed at least quarterly and upon role changes. Departing personnel lose access immediately upon offboarding. Evidence of access reviews is retained.

17. All reporting environments, data stores, and publication repositories maintain audit logs of access and change events. Logs are protected against alteration.

4.3 Reporting calendar, cut-off times, and close process

18. The Issuer maintains a documented reporting calendar with (a) Report Date cut-off times, (b) internal milestones, (c) evidence collection deadlines, (d) review and approval deadlines, and (e) external publication deadlines. The current calendar is stored in a controlled repository and changes are versioned.

19. Unless a package states otherwise, the reporting cut-off time is 23:59:59 UTC on each Report Date. If the cut-off time changes, the Issuer implements the change under documented change control and discloses it in the first package affected.

20. The close process is executed using a checklist with numbered steps, owners, timestamps, and sign-offs. The checklist template is in Schedule 2 and is completed for each monthly package.

21. The close process includes three locked stages: (a) Data Freeze, (b) Reconciliation Freeze, and (c) Publication Freeze. After each stage, the relevant dataset is checksum-sealed and stored in a write-restricted location.

22. Data Freeze means that the Issuer captures raw inputs for supply and reserves for the Report Date, stores them immutably (or in write-once storage), and records hashes. Raw inputs include: on-chain snapshots; bank and custodian statements; fund NAV statements (if any); repo confirmations (if any); and pricing files or vendor extracts used.

23. Reconciliation Freeze means that the Issuer produces the reconciliation outputs for the Report Date and finalizes the backing conclusion (Reserve Market Value ≥ FUSAUSD Token Liabilities, or not), including reconciling items. Any post-freeze changes require an exception record under Section 4.9.

24. Publication Freeze means that the Issuer finalizes the public artifacts (PDF report, data files, manifest, signatures) and performs integrity checks prior to release. After Publication Freeze, changes require a new version and correction process.

25. The Issuer retains evidence that each freeze occurred, including timestamps, file hashes, access logs, and sign-offs.

4.4 Daily controls that support monthly reporting

26. The Issuer performs daily controls intended to detect issues early and reduce month-end risk. At a minimum, daily controls include: (a) Circulating Supply verification across supported networks; (b) Reserve balance confirmations and internal ledger reconciliation; (c) limit checks under the Reserve Policy; and (d) a daily "backing check" comparing estimated Reserve Market Value to Token Liabilities.

27. Daily backing checks are measured using available intraday or prior-day pricing as applicable. The Issuer documents the limitations of daily checks and does not represent them as assurance.

28. Any material anomalies detected by daily controls are escalated immediately to the Transparency Owner, Controller, and Treasury Operations Lead, with an incident ticket opened and tracked to closure.

29. Daily control results are retained as evidence and are available to the Assurance Provider for selection as part of their testing population.

4.5 Controls over Circulating Supply and on-chain activity metrics

30. The Issuer maintains a Contract Registry listing every in-scope Token contract address by Supported Network, along with deployment metadata, admin roles, upgrade status, and canonical chain selection rules. The Contract Registry is controlled under change management (Section 4.8) and is reviewed monthly.

31. For each Supported Network, the Issuer uses at least two independent data sources to compute Circulating Supply at the cut-off time. Acceptable combinations include: (a) direct node queries + independent indexed data; (b) two independent indexers; or (c) node queries + block explorer APIs. The Issuer documents the data sources in Schedule 3.

32. The Circulating Supply calculation is performed using deterministic code with version control. The Issuer tags the code version used for each package and records the commit identifier in the internal workpapers.

33. The Issuer validates supply results by comparing: (a) total supply from contract state, (b) net minted minus net burned over time, and (c) prior period supply plus net period change. Differences outside defined tolerances must be explained and evidenced.

34. Where Supported Networks have finality uncertainty or reorg risk, the Issuer defines a finality policy (for example, a confirmation depth) and documents it in Schedule 3. Supply snapshots are taken using blocks that satisfy the finality policy.

35. The Issuer classifies and excludes internal transfers between Issuer-controlled addresses from "Minted" and "Burned" reporting, consistent with the Policy's definitions. The wallet labeling logic used for exclusions is documented and controlled.

36. If the Token is supported across multiple networks, the Issuer performs a cross-network control to ensure that the Contract Registry is complete and that no additional in-scope deployments exist outside the registry. This control includes an administrative review of deployment pipelines and known addresses.

37. The Issuer maintains an on-chain Restricted Token Register for any tokens subject to freeze, pause, blacklist, or similar controls, where such controls exist. The register records: reason code, authority action, timestamp, and current status. The Restricted Token Register is reconciled to on-chain state and disclosed in aggregate in the Transparency Package where required by the Policy.

38. If the Issuer uses bridges, wrappers, or third-party issuance mechanisms, those instruments are either (a) explicitly out of scope and labeled as such in disclosures, or (b) included only if the Issuer has full control and evidence for liabilities and supply. The Issuer does not "quietly" include third-party representations in Total Circulating Supply.

4.6 Controls over Reserve data collection and valuation

39. Reserve data is sourced directly from primary evidence. Primary evidence includes: bank statements; custodian statements; official fund administrator NAV statements; trade confirmations; repo confirmations; and independent pricing files for government instruments. Screenshots or informal emails are not used as primary evidence unless no other evidence is available, and then only with documented exception approval.

40. Each reserve account is listed in a Reserve Account Register that includes institution name, account number (masked in public materials), currency, legal title, segregation status, and permitted uses. The Reserve Account Register is reviewed monthly by the Controller and Treasury Operations Lead.

41. The Issuer performs a daily reconciliation of bank/custodian statement balances to internal reserve ledgers. For month-end, the Issuer obtains statements covering the Report Date cut-off (or the closest available statement time) and records any timing differences.

42. For government securities, the Issuer maintains a position ledger with CUSIP/ISIN identifiers, quantities, trade dates, settlement dates, maturity dates, and custodial location. The Issuer reconciles this ledger to custodian statements and trade confirmations.

43. Pricing hierarchy is defined and documented. The Issuer defines primary pricing sources and fallback sources for each asset class and documents the hierarchy in Schedule 4. Pricing overrides require Controller approval with documented rationale and evidence.

44. For money market funds (if used), the Issuer obtains official NAV statements and, where available, daily holdings or maturity summaries. The Issuer retains evidence of the fund's stated investment mandate (government-only, Reference Currency) and validates continued compliance at least quarterly.

45. For repurchase agreements (if used), the Issuer retains trade confirmations and collateral reports, including collateral type and valuation, haircuts, and unwind terms. The Issuer validates that repo collateral meets the Reserve Policy eligibility standard (government collateral only) and that the term matches the permitted term (overnight, unless explicitly permitted otherwise).

46. Reserve assets are classified into the categories disclosed in the Transparency Policy. The classification rules (including treatment of settlement-pending trades) are documented and applied consistently. Classification changes require change control and disclosure of the change.

47. The Issuer calculates WAM/WAL, maturity buckets, and liquidity tiers using documented methods. Methods are re-performed independently by a second person (or an automated independent check) at least monthly to detect formula or mapping errors.

48. The Issuer applies internal stress haircuts (if any) solely for internal risk assessment and does not apply haircuts to the public "Reserve Market Value" unless the Policy explicitly defines Reserve Market Value using such haircuts. Distinctions between accounting valuation and internal stress valuation are documented.

49. The Issuer records all reserve fees and income effects that could create reconciling items (for example, accrued interest, fund expenses, or settlement timing). The Issuer does not net reserve expenses against Token Liabilities unless the Terms and accounting basis require such treatment and it is disclosed.

4.7 Reconciliation controls and backing conclusion

50. The Issuer performs a formal reconciliation at each monthly Report Date. The reconciliation is calculated as:
- Token Liabilities (par)
- versus Reserve Market Value (fair value)
- resulting in surplus/deficit
- plus a table of reconciling items.

51. The reconciliation template is controlled and versioned. It includes: cut-off times, data sources, pricing sources, and a statement of whether Reserve Market Value is equal to or greater than FUSAUSD Token Liabilities.

52. The Controller verifies that the Token Liabilities figure matches Total Circulating Supply (as computed under Section 4.5) and that any adjustments (for example, pending redemptions) are supported by evidence.

53. The Treasury Operations Lead verifies that Reserve Market Value is supported by primary evidence. For each reserve category, the workpapers link to the underlying statements/confirmations and pricing files used.

54. A second-review control is performed for the reconciliation: a reviewer independent of preparation re-performs key calculations, checks classifications, verifies units and cut-offs, and confirms that reconciling items are described in plain, specific language.

55. The Issuer defines **tolerance thresholds** for reconciliation differences between: (a) daily internal checks and (b) the month-end reconciliation. Thresholds and escalation rules are defined in Schedule 5. Any difference exceeding the tolerance triggers escalation and a documented root-cause analysis.

56. If the Issuer cannot obtain primary evidence for a reserve component by the reporting deadline, the item is treated as an exception. Exceptions are handled as in Section 4.9 and are disclosed if they could affect a reasonable stakeholder's assessment of backing.

57. The backing conclusion (whether Reserves are ≥ liabilities) is approved by the Approver after receiving sign-offs from the Controller, Treasury Operations Lead, Blockchain Data Lead, and Security Owner as applicable.

58. The Approver's sign-off includes an explicit statement that the package reflects the final frozen dataset and that any exceptions are documented and, where required, disclosed.

4.8 Change management for reporting, definitions, and disclosures

59. Reporting code, templates, metric definitions, and disclosure formats are controlled under a change management process. Changes are categorized as: (a) minor non-substantive (formatting), (b) methodological (definition/calculation), or (c) control-relevant (affecting evidence or approvals).

60. All changes require: (i) a change request; (ii) documented rationale; (iii) peer review; (iv) testing in a non-production environment; and (v) approval by the Transparency Owner and Controller. Control-relevant changes also require Security Owner review.

61. Methodological changes require an explicit impact assessment describing the expected effect on historical series, and a disclosure plan for stakeholders. Where historical series are restated, the Issuer preserves both the old and new series and labels them clearly.

62. Emergency changes are permitted only to address a production incident, a security vulnerability, or an immediate legal requirement. Emergency changes are time-boxed, documented, and require post-implementation review and ratification within five Business Days.

63. The Issuer maintains a controlled **data dictionary** and a controlled **definitions registry** for all metrics disclosed publicly. Each metric has an owner, a definition, an extraction method, and a change log.

64. The Contract Registry and Reserve Account Register are subject to the same change control process, including monthly review and approval.

4.9 Exceptions, remediation, and evidence retention

65. An "exception" is any instance where: (a) a control step is not performed as designed, (b) primary evidence is unavailable, (c) a tolerance threshold is exceeded, or (d) a material manual override occurs.

66. Each exception is recorded in an exception log with: unique identifier, date/time, description, impacted metrics, root cause hypothesis, remediation steps, owner, due date, and closure evidence.

67. The Issuer assigns exceptions a severity level. Severity levels are based on whether the exception could affect backing conclusions, published figures, or timely redemption operations.

68. Severity levels determine escalation. High-severity exceptions are escalated immediately to the Approver and Legal/Compliance Reviewer, and are assessed for Material Event classification under the Policy.

69. Remediation is tracked to closure. Where remediation requires changes to reporting code or definitions, the change management process in Section 4.8 applies.

70. Evidence retention: the Issuer retains raw inputs, workpapers, sign-offs, logs, and published artifacts for at least 3 (three) years (or longer if required by law, regulation, or contract). Evidence is stored in a controlled repository with immutable or write-restricted retention settings.

71. The Issuer maintains an evidence index for each package, mapping each published figure to the underlying evidence and calculations.

4.10 Publication integrity controls (packaging, hashing, signing)

72. Publication artifacts are generated from the frozen dataset only. The Issuer prohibits ad-hoc manual edits to published values after Publication Freeze.

73. The Issuer produces: (a) a human-readable PDF report; (b) machine-readable data files; and (c) a manifest listing each artifact with file hash and size. The manifest is generated automatically from the artifact directory.

74. The Issuer computes SHA-256 hashes (or an equivalent cryptographic hash) for all artifacts and includes the hash list in the manifest.

75. The Issuer digitally signs the manifest and PDF report using a dedicated publication key. Publication keys are stored and used in accordance with the Issuer's key management policy, including multi-party approval for signing operations where practicable.

76. The Issuer maintains a public verification key and a key rotation plan. Key rotations are disclosed, and a transition period is used where feasible.

77. The Issuer stores the final package in at least two independent archives, one of which is write-restricted. The archive preserves historical versions and makes them retrievable.

78. Prior to publication, the Issuer performs integrity checks including: (a) verification that hashes match computed values; (b) verification of signatures; (c) cross-checking that the manifest file list

matches the published directory; and (d) a spot-check that headline figures in the PDF match the machine-readable files.

79. Publication requires dual approval: the Approver authorizes release and the Security Owner authorizes the publication key operation and confirms that sensitive details are not inadvertently disclosed.

4.11 Corrections, restatements, and incident communications

80. If the Issuer identifies a material error in a published Transparency Package, the Issuer initiates the correction process described in the Transparency Policy. The correction process produces: (a) a correction notice, (b) a corrected package version, and (c) an internal post-incident record.

81. Corrections are versioned and the prior version remains available in the archive. The Issuer labels what changed, why it changed, and whether the backing conclusion is affected.

82. If an error affects the backing conclusion or could reasonably influence redemption behavior, the Issuer escalates the matter as a potential Material Event, publishes an incident notice consistent with the Policy, and provides updates until resolution.

83. The Issuer maintains a standard correction and restatement template to ensure clarity and to avoid ambiguity around cut-off times, revised methodology, and the scope of changes.

84. All incident communications are reviewed by Legal/Compliance Reviewer prior to publication unless delay would materially increase user harm. In urgent security incidents, the Security Owner may authorize an initial notice with minimal details, followed by a fuller notice after consultation.

4.12 Third-party and vendor controls relevant to transparency

85. The Issuer identifies critical third parties that affect reporting integrity, including: reserve banks; custodians; fund administrators; pricing vendors; node providers; indexer providers; and publication hosting providers.

86. For each critical third party, the Issuer maintains: (a) due diligence records, (b) contractual SLAs and audit rights where feasible, (c) a substitution/failover plan, and (d) periodic review evidence.

87. Where a third party provides a controls report (for example, SOC reports), the Issuer reviews the report for relevant control objectives and exceptions and documents any compensating controls required.

88. If a third-party disruption impairs data availability for reporting, the Issuer records the event as an exception and assesses whether it is a Material Event under the Policy.

89. The Issuer does not rely on a single pricing source without a fallback. Fallback sources are identified and tested periodically.

4.13 Internal testing, monitoring, and continuous improvement

90. The Issuer performs periodic control testing, including evidence inspection, sampling, and re-performance. Testing is performed by internal audit, a controls function independent of process owners, or an external assessor.

91. The Issuer tracks key reporting risk indicators, including: number of exceptions per period; time to close and publish; reconciliation breaks; manual overrides; and data pipeline changes. Thresholds for escalation are defined in Schedule 5.

92. Findings from control testing are tracked in a remediation register with owners, deadlines, and closure evidence.

93. The Issuer reviews these Controls at least annually and after any Material Event that implicates reporting integrity. Updates follow change control and are disclosed where material.

Schedule 1 — RACI (minimum)
- Transparency Owner: A/R for end-to-end process, calendar, evidence index.
- Controller: A/R for valuation methods, reconciliation methodology, approvals on pricing overrides.
- Treasury Operations Lead: R for primary reserve evidence, reserve account register, daily reserve ledger reconciliation.
- Blockchain Data Lead: R for Contract Registry, supply snapshots, activity metrics, source validation.
- Security Owner: A/R for publication integrity, signing keys, access controls, security review of disclosures.
- Legal/Compliance Reviewer: A/R for incident and correction notices, regulator communications where applicable.
- Approver (CFO/CRO or delegate): A for final package approval and backing conclusion sign-off.

Schedule 2 — Close checklist (minimum)
A. Confirm Contract Registry and Reserve Account Register reviewed and approved.
B. Execute Data Freeze: capture and hash raw inputs.
C. Compute supply and activity metrics; perform independent second-source computation; resolve discrepancies.
D. Collect reserve statements, confirmations, and pricing files; validate classification and maturity mapping.
E. Compute Reserve Market Value, WAM/WAL, and liquidity tiers; perform independent re-performance.
F. Prepare reconciliation and reconciling items; apply tolerances; open exceptions as needed.
G. Draft PDF narrative; confirm figures match machine files.
H. Execute Reconciliation Freeze and Publication Freeze; record hashes and sign-offs.
I. Generate manifest, compute hashes, sign artifacts; perform integrity checks.
J. Approver sign-off; publish; archive; open post-publication review ticket.

Schedule 3 — Data sources register (template)
- Network: (insert Supported Network name; e.g., Ethereum, Base).
- Primary source: [node/indexer/vendor]
- Secondary source: [node/indexer/vendor]
- Finality policy: use a conservative finality threshold per network (defined by the Blockchain Data Lead and approved by the Controller), taking the more conservative of (i) the network's native finality mechanism and (ii) a confirmations-based rule.
- Snapshot block selection rule: use the month-end cut-off timestamp (23:59:59 UTC) and select the first block at or after that timestamp that satisfies the finality policy; record block number and hash in the manifest.

Schedule 4 — Pricing source hierarchy (template)

- Asset class: [cash / bills / notes / MMF / repo]
- Primary price source: independent pricing vendor feed (or official fund administrator NAV for MMFs), recorded in the valuation workbook with source identifiers.
- Secondary price source: independent secondary vendor or broker quote; if unavailable, use the prior day's validated price and treat as an exception.
- Override approvals: [Controller]
- Evidence required: source statement or vendor extract, timestamped and archived; for cash, bank statements; for securities, custodian statements and pricing vendor output; for MMFs, official NAV statement and holdings/price report.

Schedule 5 — Tolerances and escalation (template)

- Supply discrepancy tolerance (primary vs secondary): the greater of 10 tokens or 0.0001%.
- Daily vs month-end backing estimate tolerance: 0.05%.
- Reconciliation break threshold for escalation: USD 10,000 (absolute) and 0.01% (relative).
- Publication deadline variance threshold: 3 Business Days.
- Exception severity rules: Low (formatting / immaterial rounding), Medium (single evidence gap or valuation override without impact to backing conclusion), High (any change that could affect the backing conclusion, any reserve coverage shortfall, or any control failure requiring a correction notice).