Meridion Risk Assessment: Tether USD (USDT)

FIELD	VALUE
Digital Asset	Tether USD (USDT)
Risk Areas	Smart Contract, Operations, Financials
Chains	Ethereum Mainnet (Chain ID: 1)
Report Version	1.0.0
Assessment Period	2026-04-23 to 2026-05-06
Date of Publication	2026-05-08
Requested by	Non-issuer

1. Methodology

1.1 Rating Standard and Assessment Framework

This report is produced under the **Meridion Risk Rating Standard v1**. The engagement was conducted by a team combining smart contract security specialists, financial risk analysts, and formal methods engineers.

Each independent domain receives a risk rating of **Low**, **Medium**, or **High**:

- **Low** applies when no material adverse condition was identified within the assessed scope and residual risks are ordinary for the asset type.
- **Medium** applies when a material weakness, dependency, opacity, concentration, or stress scenario exists but is contingent, mitigated, not currently causing holder harm, or primarily a future-risk driver.
- **High** applies when a direct or credible path exists to material holder loss, unauthorized issuance, severe depeg, impaired transferability, asset shortfall or misrepresentation, governance or administrator capture, or operational failure.

The composite risk rating is derived from the three domain ratings using the following labels:

- **Minimal:** all three domain ratings are Low, with no material identified weakness beyond ordinary residual risk for the asset type.
- **Low:** no domain rating reaches High, and at most one reaches Medium; any Medium condition is isolated or future-oriented, with no immediate consequence for holders.
- **Moderate:** no domain rating reaches High, but multiple domains carry a Medium rating, or one Medium domain carries direct consequence, structural importance, or meaningful interaction with another domain.
- **Elevated:** at least one domain rating reaches High, but the condition remains contingent, is not actively causing holder harm, and does not currently show immediate adverse consequences.
- **High:** immediate adverse consequences are present, or an identified High domain condition bears directly on holders.

- **Severe:** multiple domains are critically compromised, or a single compromised domain produces cascading failure across the asset.

Each domain and the composite conclusion also receive a confidence rating of **Low**, **Medium**, or **High**. Confidence measures the reliability, completeness, independence, recency, and reproducibility of the evidence supporting the risk rating. Confidence does not reduce or soften the risk rating; instead, it tells the reader how strongly the rating is supported and whether material scope limitations reduce certainty.

1.2 Review Techniques Applied

SMART CONTRACTS: FUNCTIONALITY AND SECURITY

- **Runtime entry-point catalogue:** reconstruction of the complete externally callable runtime surface from deployed bytecode and verified source artifacts
- **Manual code review:** line-by-line inspection of all in-scope source files by independent security specialists
- **Edge-case and exploit-negative review:** targeted analysis of protocol-specific invariants, failure modes, access-control boundaries, replay protections, and upgrade assumptions
- **Formal verification:** direct deployed-bytecode verification of hidden calldata surface, covering selectors outside the complete runtime catalogue and malformed calldata shorter than 4 bytes
- **Fork-based behavioral testing:** live-chain execution of representative positive and negative behavioral tests against deployed bytecode using Foundry; test counts, entry-point coverage, and PASS/FAIL status are reported in the bytecode assurance section
- **AI-assisted analysis:** automated pattern detection and anomaly scanning across the full codebase to supplement human review

OPERATIONS: KEY MANAGEMENT AND ADMINISTRATIVE CONTROL

- **Role mapping:** reconstruction of deployment and administrative authority from on-chain state and historical events
- **Key management review:** assessment of HSM, MPC, and key ceremony controls based on SOC reports and public disclosures
- **Monitoring and alerting:** assessment of on-chain event alerting coverage and anomaly detection arrangements for privileged operations and administrative actions
- **Recovery assessment:** review of signer loss, compromise, and administrative recovery procedures

FINANCIALS: UNDERLYING ASSETS AND COUNTERPARTIES

- **Reserve attestation analysis:** comparison of attestation disclosures against on-chain liabilities and supply metrics
- **Counterparty profiling:** identification of issuer, custodian, banking, and attestation dependencies and their risk posture
- **Liquidity analysis:** assessment of redemption capacity and market depth across DEX and CEX venues
- **Scenario analysis:** review of economic stress scenarios and their implications for solvency, redemptions, and price stability.

2. Executive Summary

Subject Overview

Tether USD (USDT) is a fiat-referenced stablecoin issued by Tether International, S.A. de C.V. It is designed to maintain a 1:1 peg to the US dollar and is backed by a reserve comprising primarily short-duration US Treasury bills, along with gold, Bitcoin, and other assets. USDT is the world's largest stablecoin by market capitalization and serves as the dominant base trading pair across centralized and decentralized crypto exchanges globally. At the assessment snapshot (block 24,941,472, 2026-04-23), the on-chain supply on Ethereum Mainnet was approximately 98.08 billion USDT. Market-reported circulating supply across all chains was approximately 189.59 billion USDT, representing a total market capitalization of approximately $189.5 billion. The TetherToken contract was deployed in November 2017 and has not been upgraded, deprecated, or paused since deployment.

KYC Gating

Secondary-market holding and transfer of USDT requires no KYC; tokens move freely on-chain subject only to Tether's blacklist mechanism. Minting is conducted exclusively by the contract owner (Tether's 3-of-6 Gnosis Safe multisig) via the `issue(uint256)` function; no third-party address may mint. Direct redemption of USDT for USD through Tether's platform requires full KYC/AML verification and is available only to verified institutional participants; the minimum redemption threshold is $100,000 USD, a fee of the greater of $1,000 or 0.1% applies, and settlement is conducted during business banking hours (not 24/7). Retail holders cannot directly redeem and must access liquidity via secondary markets. At the on-chain level, compliance is enforced through a blacklisting mechanism controlled by the owner: `addBlackList(address)` blocks a designated address from calling `transfer()`, and `destroyBlackFunds(address)` permanently burns the balance of a blacklisted address. As of the assessment snapshot, 2,919 addresses have been added to the blacklist and 288 subsequently removed. Tether cooperates actively with OFAC, DOJ, and other authorities on sanctions and AML enforcement through this mechanism.

Overall Risk Rating: Moderate

Composite Confidence: Medium

The two most significant risk dimensions for USDT are operational transparency and liquidity structure. On the operational side, while the contract owner is a 3-of-6 Gnosis Safe multisig that prevents single-key compromise from enabling unilateral privileged actions, Tether has not publicly disclosed its individual signer key management arrangements, incident response procedures, or monitoring policy, and no SOC 2 or equivalent independent assurance is available. On the financial side, the Q1 2026 BDO attestation confirms 104.5% collateralization ($191.77B in assets against $183.54B in liabilities), with a $8.23B excess reserve buffer; however, direct redemption is institutionally gated and functionally unavailable to retail holders at scale, and a 25% mass-exit scenario within six hours would exceed all available liquidity channels and cause material secondary-market peg dislocation. USDT is also non-compliant with MiCA in the EU, and an unresolved DOJ investigation represents a regulatory tail risk. Smart contract risk is low: the deployed contract has no exploitable vulnerabilities, two low-severity findings, and formal verification confirmed no hidden trapdoor selectors. Composite confidence is Medium, reflecting the limited assurance standard of the BDO attestation, undisclosed custodian identities, and undisclosed operational security arrangements.

Smart Contract Security Summary

SEVERITY	COUNT	RESOLVABLE
Critical	0	0
High	0	0
Medium	0	0
Low	2	2

The smart contract security review identified two Low-severity findings. SEC-01 describes a single-step ownership transfer pattern in `transferOwnership()` that could irrecoverably lose all administrative control if the new owner address is unreachable; mitigation via a two-step pattern is recommended. SEC-02 documents an asymmetric blacklist enforcement gap in `transferFrom()`, which does not check whether the caller (`msg.sender`) is blacklisted, unlike `transfer()` ; a blacklisted address holding a prior allowance can exploit this asymmetry to act as a spender on approved non-blacklisted funds. Neither finding creates an exploitable path for unauthorized fund extraction by unprivileged parties without preconditions controlled by the multisig owner or by a prior allowance. Formal verification confirmed that all unknown 4-byte selectors and short calldata inputs always revert on the deployed bytecode, with no hidden trapdoor paths. The contract's overall control posture is conservative: SafeMath arithmetic, payload-size guards against short-address attacks, pause and blacklist gating on transfers, and a bounded fee mechanism.

Smart Contract Risk Score: Low | Confidence: High

Operational Security Summary

The contract owner is a 3-of-6 Gnosis Safe multisig (`0xc6cde7c39eb2f0f0095f41570af89efc2c1ea828`), which prevents any single key compromise from enabling unilateral privileged actions including minting, burning, pausing, blacklisting, deprecating, or transferring ownership. No ownership transfers, pauses, or deprecation events have been recorded in over eight years of operation since the November 2017 deployment. However, all privileged operations execute immediately in a single transaction with no timelock; the deprecation mechanism is irreversible and accepts any address without validation; and individual signer key management, monitoring policy, and incident response procedures are not publicly disclosed. No SOC 2 or equivalent independent operational security assurance is publicly available. An adverse finding in undisclosed off-chain controls could change this rating.

Opsec Risk Score: Medium | Confidence: Medium

Financial Summary

Tether's Q1 2026 BDO attestation confirms $191.77B in consolidated assets against $183.54B in liabilities, a collateralization ratio of 104.5% with a $8.23B excess reserve buffer. The reserve composition is dominated by short-duration US Treasury bills (approximately 73.5% of assets), which limits duration and credit risk and enables rapid partial liquidation via repo under normal conditions. The attestation uses an ISAE 3000 limited assurance standard rather than a full audit; material custodian identities for T-bill, gold, and Bitcoin holdings are not publicly disclosed; and multi-chain USDT supply was not independently reconciled. Direct redemption

is institutionally gated ($100K minimum, KYC required, T+1 settlement), making large-scale retail exits dependent on secondary-market liquidity. USDT's non-compliance with MiCA results in ongoing de-listing pressure at EU-regulated venues, and an unresolved DOJ investigation represents a regulatory tail risk.

Financial Risk Score: Medium | Confidence: Medium

Scope Limitations

- **Multi-chain USDT supply not independently reconciled:** Approximately 91.5 billion USDT circulating on Tron, BNB Smart Chain, Solana, and other chains was not independently verified on-chain. This assessment relies on market-reported circulating supply data. Affects confidence in cross-chain financial supply assurance.
- **Custodian identities undisclosed:** Material custodian identities for T-bill, gold, and Bitcoin reserve assets are not publicly disclosed, preventing independent verification of asset segregation quality. Affects confidence in the financial domain and prevents an upgrade above Medium confidence.
- **Off-chain operational controls undisclosed:** Individual signer key management, incident response playbook, and monitoring policy are not publicly documented. Affects confidence in the operational security domain and prevents an upgrade above Medium confidence.
- **Non-Ethereum USDT deployments not assessed:** USDT deployments on Tron, BNB Smart Chain, Solana, and other chains are outside the scope of this report. No rating effect for this Ethereum-focused engagement; any adverse condition on another chain could affect total supply integrity. Affects confidence in the financial domain.

3. Part I: Smart Contract Security Analysis

Smart Contract Security Rating: Low | Confidence: High

3.1 Scope and Execution Environment

Chain: Ethereum Mainnet

Assessment snapshot block: 24,941,472 (2026-04-23)

CONTRACT	ROLE	ADDRESS	COMPILER	VERIFIED
TetherToken	Token	`0xdAC17F958D2ee523a2206206994597C13D831ec7`	`v0.4.18+commit.9cf6e910`	Yes

TetherToken is a self-contained single-file contract that does not use a delegatecall-based proxy. It implements a custom call-forwarding "deprecation" mechanism that routes ERC-20 calls via plain `CALL` to an upgraded address when activated; however, as of the assessment snapshot, the `deprecated` flag is `false` and no upgraded address has ever been set. Source code is verified on Etherscan and matches the deployed bytecode. No implementation contract exists separately; the Token entry in the table above represents the full scope of in-scope bytecode.

3.2 Entry Point Catalogue

The following table lists only state-modifying, externally reachable entry points. View and pure functions are excluded from display but used in the formal verification runtime.

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
EP-001	`transfer(address,uint256)`	Public	High	Transfers tokens from `msg.sender` to `_to`. Reverts if paused or if `msg.sender` is blacklisted. Applies the current fee (0 basis points) and routes to `upgradedAddress` when deprecated. Guards against short-address attacks via `onlyPayloadSize(64)`.
EP-002	`transferFrom(address,address,uint256)`	Public	High	Transfers tokens from `_from` to `_to` using `msg.sender`'s pre-approved allowance. Checks `_from` blacklist status but does NOT check `msg.sender` blacklist status (SEC-02). Supports MAX_UINT infinite-approval sentinel. Routes to `upgradedAddress` when deprecated.
EP-003	`addBlackList(address)`	`onlyOwner`	Medium	Adds `_evilUser` to the `isBlackListed` mapping, blocking them from calling `transfer()` and enabling `destroyBlackFunds()` against them.
EP-004	`approve(address,uint256)`	Public	Medium	Sets `msg.sender`'s allowance for `_spender`. Enforces a zero-first pattern to mitigate the ERC-20 approval race condition. Callable when paused. Routes to `upgradedAddress` when deprecated.
EP-005	`deprecate(address)`	`onlyOwner`	Medium	Activates call-forwarding by setting `deprecated=true` and

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
				recording `upgradedAddress`. Irreversible; no zero-address check. Causes all subsequent ERC-20 state calls to be forwarded via plain `CALL` to the new contract.
EP-006	`destroyBlackFunds(address)`	`onlyOwner`	Medium	Seizes and permanently burns all tokens held by a blacklisted address, decrementing total supply by the same amount. Requires the target to already be blacklisted.
EP-007	`issue(uint256)`	`onlyOwner`	Medium	Mints `amount` new tokens into the owner's balance and increments total supply. Overflow-guarded via explicit `require` checks.
EP-008	`pause()`	`onlyOwner`	Medium	Sets `paused=true`, blocking all `transfer()` and `transferFrom()` calls globally. Requires the contract to currently be unpaused.
EP-009	`redeem(uint256)`	`onlyOwner`	Medium	Burns `amount` tokens from the owner's balance and decrements total supply. Underflow-guarded via explicit `require` checks.
EP-010	`setParams(uint256,uint256)`	`onlyOwner`	Medium	Sets the transfer fee rate (`basisPointsRate`, max 19) and the absolute fee cap (`maximumFee`, max 49 USDT-units). Both parameters are currently 0.
EP-011	`removeBlackList(address)`	`onlyOwner`	Low	Removes `_clearedUser` from the `isBlackListed` mapping, restoring their

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
				ability to call `transfer()`.
EP-012	`transferOwnership(address)`	`onlyOwner`	Low	Transfers contract ownership to `newOwner` in a single step with no confirmation (SEC-01). Silently ignores `address(0)` but does not protect against other invalid addresses.
EP-013	`unpause()`	`onlyOwner`	Low	Sets `paused=false`, restoring `transfer()` and `transferFrom()`. Requires the contract to currently be paused.

An additional 19 view and pure functions are also part of the runtime surface, they are read-only and carry no independent risk.

3.3 Bytecode Surface Attestation

As capital held in on-chain assets grows, the Solidity compiler (`solc`) and deployment pipeline become increasingly attractive supply-chain attack targets. A compromised compiler, build process, or deployment artifact could insert hidden trap doors that are not visible in source-level review but are present in deployed bytecode. Meridion therefore separates bytecode assurance into two complementary controls: formal verification of hidden calldata surface and fork-based behavioral tests of intended entry-point behavior on deployed bytecode.

Input artefact hashes (Keccak-256 of deployed bytecode):

CONTRACT	ROLE	ADDRESS	BYTECODE HASH (KECCAK-256)
TetherToken	Token	`0xdAC17F958D2ee523a2206206994597C13D831ec7`	`0xb44fb4e949d0f78f87f79ee46428f23a2a57`

Verification engine: The *Meridion Formal Verification Engine v1* is a custom-built symbolic execution environment executing EVM bytecode that supports JUMPI-tracing and SMT solving to verify the absence of trapdoors.

3.3.1 HIDDEN-SURFACE FORMAL VERIFICATION

The complete entrypoint catalogue (EP-001 through EP-032, covering all 32 runtime-reachable function selectors) was used as the exclusion set for hidden-surface verification. Note that the report table in Section 3.2 lists only the 13 state-mutating functions; the 19 view and pure functions are excluded from that table but are included in the full exclusion set used for formal verification.

TetherToken: Bytecode Surface Cases

Formal verification of the deployed TetherToken bytecode confirmed the following hidden-surface behavior:

CASE	CONSTRAINT	CLASSIFICATION	VERDICT
Unknown 4-byte selectors	selector not in the complete runtime selector catalogue	always reverts	CONFIRMED
Short calldata	calldata_size < 4	always reverts	CONFIRMED

Overall verdict: CONFIRMED

All feasible execution paths for unknown selectors and short calldata terminate in a revert. No unexpected non-reverting hidden selector path was found. TetherToken uses the standard Solidity 0.4.x dispatcher, which reverts on unrecognized selectors by falling through without a payable fallback handler. No delegatecall instructions are present in the bytecode.

3.3.2 FORK-BASED BEHAVIORAL TESTS

Fork-based behavioral tests were executed against the deployed TetherToken address `0xdAC17F958D2ee523a2206206994597C13D831ec7` on an Ethereum mainnet Foundry fork at the assessment snapshot block 24,941,472. Tests used `vm.prank` to simulate owner-gated calls from the 3-of-6 Gnosis Safe multisig owner (`0xC6CDE7C39eB2f0F0095F41570af89eFC2C1Ea828`).

ENTRY POINT	FUNCTION	POSITIVE TEST	NEGATIVE TEST
EP-001	`transfer`	PASS: succeeds for a non-blacklisted sender with sufficient balance	PASS: reverts for a blacklisted sender
EP-002	`transferFrom`	PASS: succeeds with valid allowance and balance	PASS: reverts when `_from` is blacklisted
EP-003	`addBlackList`	PASS: owner adds a target address to the blacklist	PASS: non-owner call reverts
EP-004	`approve`	PASS: succeeds for any caller while unpaused or paused	N/A: no required negative case in the test plan
EP-005	`deprecate`	PASS: owner can set `deprecated` and `upgradedAddress` on a snapshot/revert fork	PASS: non-owner call reverts
EP-006	`destroyBlackFunds`	PASS: owner destroys the balance of a blacklisted address	PASS: non-owner call reverts
EP-007	`issue`	PASS: owner mints new USDT to the owner balance	PASS: non-owner call reverts
EP-008	`pause`	PASS: owner pauses transfers globally	PASS: non-owner call reverts
EP-009	`redeem`	PASS: owner burns USDT from the owner balance	PASS: non-owner call reverts
EP-010	`setParams`	PASS: owner updates fee parameters	PASS: non-owner call reverts
EP-011	`removeBlackList`	PASS: owner removes a previously blacklisted address	PASS: non-owner call reverts
EP-012	`transferOwnership`	PASS: owner transfers ownership on a snapshot/revert fork	PASS: non-owner call reverts
EP-013	`unpause`	PASS: owner restores transfers after a pause	PASS: non-owner call reverts

An optional fork smoke test for a selector outside the runtime catalogue was not run and was not counted as a required case; formal verification remains the authoritative hidden-surface control.

Fork-test overall result: PASS (25/25 required cases passed; 13 positive cases, 12 negative cases, all 13 state-mutating entry points exercised)

3.3.3 BYTECODE ASSURANCE CONCLUSION

Formal verification and fork testing answer different questions. Formal verification provides exhaustive assurance over hidden calldata surface within its modeled constraints: unknown selectors and malformed short calldata. Fork tests provide sampled behavioral assurance that the deployed bytecode performs representative intended operations and rejects representative invalid operations.

Formal verification is CONFIRMED: all hidden-surface cases revert, and no unexpected non-reverting path exists in the deployed bytecode. Fork-based behavioral tests are PASS: 13 positive tests and 12 negative tests all passed against the live-fork bytecode, covering all 13 state-mutating entry points. The full combined bytecode-assurance claim is made for the TetherToken deployment. Formal verification provides exhaustive assurance over hidden calldata surface; fork tests provide sampled behavioral assurance that the deployed bytecode performs expected operations and rejects unauthorized operations on live chain state.

3.4 Edge-Case Analysis

Edge-case analysis was conducted independently by a human security researcher and advanced AI tooling for all Critical and High entry points using line-by-line source code review. Key findings are summarised below.

EDGE CASE	STATUS	EVIDENCE
Zero-value `transfer()`	Safe	`SafeMath.sub(balance, 0)` and `.add(0)` succeed; fee calculation yields 0; transfer completes normally with event emitted
Short-address attack on `transfer()`	Mitigated	`onlyPayloadSize(64)` guard reverts calls with fewer than 68 bytes (4-byte selector plus 64 argument bytes) before any state change
Short-address attack on `transferFrom()`	Mitigated	`onlyPayloadSize(96)` guard reverts calls with fewer than 100 bytes before any state change
Reentrancy via deprecated call-forwarding in `transfer()`	Mitigated	All balance updates complete before the forwarding call; the forwarded `CALL` cannot exploit this contract's already-unchanged storage
Reentrancy via deprecated call-forwarding in `transferFrom()`	Mitigated	Same reasoning as `transfer()`; checks-effects-interactions ordering maintained
Pause-state `transfer()`	Mitigated	`whenNotPaused` modifier reverts if `paused==true`; `approve()` remains callable by design
Blacklisted sender calling `transfer()`	Mitigated	`require(!isBlackListed[msg.sender])` reverts
Blacklisted spender calling `transferFrom()`	Unsafe	Finding SEC-02: `transferFrom()` does not check `msg.sender` blacklist status; a blacklisted address with a prior approval can move approved funds
MAX_UINT infinite-approval sentinel in `transferFrom()`	Safe	Allowance is not decremented when `allowed[_from][msg.sender] == MAX_UINT`; this is intentional design
Transfer to zero address via `transfer()`	Safe	Permitted by design; tokens sent to `address(0)` are effectively burned; no revert occurs
Overflow in `transfer()` balance arithmetic	Mitigated	`SafeMath` guards all balance additions and subtractions; overflows revert

3.5 Common Exploit Negatives

Based on line-by-line source code review by human security researchers and LLM-based reasoning, the following exploit negatives were identified:

EXPLOIT CLASS	STATUS	EVIDENCE
Reentrancy	Mitigated	Checks-effects-interactions maintained; no external calls to untrusted contracts in the non-deprecated path; deprecated call-forwarding cannot exploit this contract's already-finalized state
Integer overflow / underflow	Mitigated	`SafeMath` applied to all balance arithmetic; `issue()` and `redeem()` use `require`-based guards equivalent to `SafeMath`; `destroyBlackFunds()` raw subtraction is safe by the supply invariant (sum of balances equals total supply)
Access control bypass	Mitigated	All privileged functions protected by `onlyOwner` modifier consistently applied; no bypass paths identified
Front-running	Mitigated	Approve race condition mitigated by the zero-first pattern in `approve()`; no price-sensitive logic in transfer operations
Oracle manipulation	Not applicable	TetherToken contains no on-chain oracle dependency and performs no price computation
Signature replay	Not applicable	No signature verification logic; no `ecrecover` calls; no EIP-712 domain; authorization is via `msg.sender` checks and on-chain allowance state
Flash loan attack	Not applicable	No price-sensitive operation exists in this contract that flash loans could exploit
Denial of service	Not applicable	All entry points are O(1) in gas consumption; no unbounded loops or user-controlled iteration present

3.6 Security Findings Register

SEC-01: SINGLE-STEP OWNERSHIP TRANSFER WITHOUT CONFIRMATION

FIELD	DETAIL
Finding ID	SEC-01
Title	Single-step ownership transfer without confirmation
Severity	Low
Entry Point(s)	EP-012 (`transferOwnership(address)`)
Description	`transferOwnership(address newOwner)` immediately sets `owner = newOwner` in a single transaction with no two-step confirmation. If `newOwner` is a mistyped or unreachable address, ownership is irrecoverably lost and all `onlyOwner` -gated functions become permanently inaccessible. The `address(0)` edge case is silently ignored rather than reverted, which prevents the null-address scenario but does not protect against other invalid addresses.
Impact	Permanent loss of all administrative control over the contract if the new owner address is unreachable. No on-chain recovery path exists. All privileged functions (issue, redeem, pause, unpause, addBlackList, removeBlackList, destroyBlackFunds, deprecate, setParams, transferOwnership) become permanently inaccessible.
Recommendation	Adopt a two-step ownership transfer pattern: `transferOwnership()` stores a `pendingOwner` slot without immediately updating `owner` , and a separate `acceptOwnership()` call restricted to `pendingOwner` finalises the transition. This ensures the new owner key is accessible before the transition is committed.

SEC-02: ASYMMETRIC BLACKLIST ENFORCEMENT IN `TRANSFERFROM()`

FIELD	DETAIL
Finding ID	SEC-02
Title	Asymmetric blacklist enforcement: `transferFrom()` does not check caller blacklist status
Severity	Low
Entry Point(s)	EP-002 (`transferFrom(address,address,uint256)`)
Description	`transfer()` checks `require(!isBlackListed[msg.sender])`, blocking blacklisted addresses from initiating token flows on their own behalf. `transferFrom()` checks `require(!isBlackListed[_from])`, blocking flows from blacklisted source addresses, but does NOT check whether `msg.sender` is blacklisted. A blacklisted address that holds or obtains a prior allowance from a non-blacklisted account can call `transferFrom()` as the spender to move those approved tokens. This creates an asymmetry in the regulatory freeze mechanism.
Impact	A blacklisted address can initiate `transferFrom()` on approved non-blacklisted accounts, partially circumventing the intended scope of the blacklist. The blacklisted user cannot extract or move their own frozen tokens through this path; the impact is limited to approved third-party funds where an allowance exists.
Recommendation	Add `require(!isBlackListed[msg.sender])` to `transferFrom()` alongside the existing `require(!isBlackListed[_from])` check. This aligns blacklist enforcement semantics between `transfer()` and `transferFrom()` and prevents blacklisted addresses from acting as spenders on any approved flows.

4. Part II: Operational Security

Operational Security Rating: Medium | Confidence: Medium

4.1 Privileged Roles

Role holders at assessment snapshot:

ROLE	ADDRESS	TYPE
owner	`0xc6cde7c39eb2f0f0095f41570af89efc2c1ea828`	Multisig (Gnosis Safe, 3-of-6)

TetherToken exposes a single privileged role: `owner`. There is no role separation; one address governs every administrative function simultaneously. The `owner` is held by `0xc6cde7c39eb2f0f0095f41570af89efc2c1ea828`, confirmed as a contract by on-chain inspection (`eth_getCode`), labeled "Tether: Multisig" on Etherscan, and independently identified as a Gnosis Safe with a 3-of-6 threshold. No secondary guardian, emergency role, or backup governance contract exists. The zero address does not hold any privileged role.

Powers conferred by the owner role:

- **Mint:** `issue(uint256)` (EP-007) creates new USDT credited to the owner address, increasing total supply.
- **Burn:** `redeem(uint256)` (EP-009) destroys USDT from the owner address, decreasing total supply.
- **Pause/Unpause:** `pause()` (EP-008) / `unpause()` (EP-013) halts or restores all `transfer()` and `transferFrom()` calls globally with immediate effect.
- **Blacklist management:** `addBlackList(address)` (EP-003) / `removeBlackList(address)` (EP-011) blocks or unblocks individual addresses from sending tokens.
- **Destroy blacklisted funds:** `destroyBlackFunds(address)` (EP-006) permanently burns a blacklisted address's entire token balance.
- **Deprecate/upgrade:** `deprecate(address)` (EP-005) activates irreversible call-forwarding to a new contract; no input validation is applied.
- **Fee setting:** `setParams(uint256,uint256)` (EP-010) activates or adjusts the transfer fee (currently 0 basis points, bounded at a maximum of 19 basis points and 49 USDT-units absolute cap).
- **Ownership transfer:** `transferOwnership(address)` (EP-012) reassigns the owner role in a single step with no confirmation (SEC-01).

All functions are gated by `onlyOwner` and execute in a single transaction with no delay. The 3-of-6 multisig threshold means any privileged action requires three of the six signers to agree. Individual signer key management arrangements (HSM, MPC, hardware wallet) are not publicly disclosed.

4.2 Administration History

Ownership Changes: No `OwnershipTransferred` events appear in the on-chain event history. The owner address `0xc6cde7c39eb2f0f0095f41570af89efc2c1ea828` has been the TetherToken owner since deployment in November 2017, a continuous tenure of over eight years with no rotation.

Pause Events: No `Pause` or `Unpause` events appear in the event history. The contract has never been paused on Ethereum Mainnet as of the assessment snapshot.

Upgrade and Deprecation Events: No `Deprecate` events appear in the event history. The `deprecated` flag is `false`. The contract has never been upgraded or migrated since its 2017 deployment.

Blacklist Activity: Blacklisting is the most frequently exercised administrative function:

EVENT	COUNT	DATE RANGE
`AddedBlackList`	2,919	November 2017 to April 2026
`RemovedBlackList`	288	2018 to April 2026

The most recent blacklist events in the snapshot are dated April 23, 2026. Activity is continuous and routine. Early events (December 2018) include blacklisting of `address(0)` and several low-ordinal addresses, which appear to be defensive pre-emptive blocks rather than sanctions responses. Tether has publicly documented freezing approximately $4.2 billion in USDT since inception and $3.5 billion since 2023. In September 2024, Tether co-founded the T3 Financial Crime Unit with TRON and TRM Labs; this consortium froze over $300 million in criminal assets within its first year of operation.

Fee Mechanism: The `setParams` function has never been used. Both `basisPointsRate` and `maximumFee` are currently 0. No fee has ever been activated in the contract's history. The owner could activate fees at any time with no advance notice.

4.3 Upgrade Risk Analysis

Proxy Standard: TetherToken uses a custom call-forwarding deprecation mechanism, not a standard delegatecall-based proxy. This was confirmed by source inspection and bytecode analysis. No `delegatecall` instructions are present in the bytecode, no EIP-1967 slots are used, and the `upgradeTo` / `upgradeToAndCall` selectors are absent from the ABI.

Upgrade Mechanism: The owner can call `deprecate(address _upgradedAddress)` (EP-005), which: (1) sets `deprecated = true`; (2) records `upgradedAddress = _upgradedAddress`; and (3) causes all subsequent calls to `transfer`, `transferFrom`, `approve`, `balanceOf`, `allowance`, and `totalSupply` to forward via plain `CALL` to the upgraded contract. This is a migration aid, not a live delegatecall proxy. The original contract retains its own storage; the new contract operates independently with its own separate storage.

No Timelock: The owner can trigger deprecation in a single transaction with no delay, no governance vote, and no confirmation requirement beyond the 3-of-6 multisig threshold. Token holders receive no advance notice.

Storage Layout Risk: Not applicable. Because call-forwarding uses plain `CALL`, the new contract has its own independent storage. There is no shared storage context and therefore no storage collision or layout-incompatibility risk.

Initialisation Risk: Not applicable. There is no delegatecall-based initialisation pattern, no `initialize()` function, and no re-initialisation vector.

Practical Implications for Token Holders: Deprecation is irreversible; no `undeprecate()` function exists. The target address passed to `deprecate()` is not validated (no zero-address check, no interface check); an incorrect address would brick all ERC-20 operations on the legacy contract immediately and permanently. The new contract must implement the `UpgradedStandardToken` interface (`transferByLegacy`, `transferFromByLegacy`, `approveByLegacy`) for ERC-20 forwarding to function. The blacklist on the original contract continues to gate `transfer` / `transferFrom` even in deprecated mode; the upgraded contract does not automatically inherit the existing blacklist state.

4.4 Recovery Scenarios

Recovery analysis is constrained by the lack of public disclosure of Tether's key management, incident response, or recovery procedures.

SCENARIO 1: ONE OR TWO SIGNER KEYS LOST

FIELD	DETAIL
Detection Method	Tether internal signer availability monitoring (undisclosed); privileged transaction fails to reach quorum; signer becomes unresponsive
Recovery Possible?	Yes
Recovery Authority	Remaining Gnosis Safe signers (at least 3 of remaining 4-5 must be available)
Recovery Path	Remaining signers reach quorum and call `swapOwner()` on the Gnosis Safe to replace the lost signer addresses with new signer addresses
Prerequisites / Dependencies	At least 3 of the remaining signers are available with functioning key material; new signer keys are available; Ethereum network is operational
Operational Impact	Reduced signer diversity during the recovery period; privileged contract operations remain available if quorum is maintained
Residual Risk	Identity and key management of replacement signers are not publicly disclosed; reduced signer count before rotation increases exposure temporarily

SCENARIO 2: MULTISIG QUORUM LOST (4 OR MORE OF 6 SIGNERS UNAVAILABLE)

FIELD	DETAIL
Detection Method	Privileged transaction proposals fail to accumulate 3 approvals over an extended period; operations team observes quorum failure
Recovery Possible?	No
Recovery Authority	None: the Gnosis Safe contract enforces the 3-of-6 threshold on-chain with no override mechanism
Recovery Path	No on-chain recovery path. TetherToken becomes administratively frozen: no new mints, burns, pauses, blacklist changes, or ownership transfers are possible. The existing token supply and state persist unchanged.
Prerequisites / Dependencies	N/A
Operational Impact	All privileged operations permanently unavailable. USDT effectively becomes an immutable token with fixed supply. Law enforcement blacklist compliance impossible.
Residual Risk	Extreme: permanent loss of administrative control over the world's largest stablecoin. No contractual or on-chain mechanism for recovery.

SCENARIO 3: ACCIDENTAL PROTOCOL PAUSE

FIELD	DETAIL
Detection Method	Immediate: all USDT transfers on-chain revert; user reports and monitoring dashboards detect transfer failures within minutes
Recovery Possible?	Yes
Recovery Authority	Tether Multisig (3-of-6)
Recovery Path	Owner calls `unpause()` to restore transfer functionality; no timelock or delay applies
Prerequisites / Dependencies	At least 3 signers available to approve the unpause transaction; Ethereum network operational
Operational Impact	All USDT transfers globally halted for the duration of the pause. DeFi protocols, exchanges, and payment systems disrupted. Duration depends on signer availability and coordination speed.
Residual Risk	Low: unpause capability is equivalent to pause capability; recovery can be immediate once quorum is assembled

SCENARIO 4: FAILED DEPRECATION (WRONG TARGET ADDRESS SUPPLIED)

FIELD	DETAIL
Detection Method	Post-execution: all ERC-20 calls begin returning incorrect results or reverting; monitoring dashboards, DEX integrations, and wallets immediately detect failures
Recovery Possible?	No
Recovery Authority	No on-chain recovery authority; deprecation is irreversible with no `undeprecate()` function
Recovery Path	A new correct contract must be deployed and announced. All exchanges, wallets, DeFi protocols, and holders must voluntarily migrate to the new address. This is a voluntary, ecosystem-wide coordination process with no on-chain enforcement mechanism.
Prerequisites / Dependencies	Deployment of a new replacement contract; broad ecosystem coordination across exchanges, wallets, DeFi protocols, and custodians; Tether's ability to credibly announce the new canonical address
Operational Impact	Severe and immediate: all ERC-20 operations on the original TetherToken contract are permanently non-functional. Market disruption likely severe given USDT's role as the largest stablecoin.
Residual Risk	High: migration to a new address is voluntary and may be slow or incomplete; some holders may remain stranded on the bricked contract

SCENARIO 5: FEWER THAN 3 MULTISIG SIGNERS COMPROMISED

FIELD	DETAIL
Detection Method	Anomalous or unauthorized transaction proposals appearing in the Gnosis Safe pending transaction queue; external on-chain monitoring of Safe proposal activity
Recovery Possible?	Yes
Recovery Authority	Remaining honest signers (at least 3 uncorrupted signers of the 6)
Recovery Path	Honest signers reject malicious proposals and use their quorum to call `swapOwner()` to remove compromised signer addresses and replace them with new secure keys
Prerequisites / Dependencies	Compromise is detected before malicious proposals accumulate 3 approvals; at least 3 honest signers are available and coordinated; new signer key material is available
Operational Impact	Temporary operational disruption while compromised signers are rotated out; if malicious proposals accumulated 3 approvals before detection, unauthorized actions may have executed
Residual Risk	Medium: if 3 or more signers are simultaneously compromised, full owner privilege is available to the attacker, including the irreversible `deprecate()` function

SCENARIO 6: COMPROMISED SIGNING INFRASTRUCTURE OR OPERATIONAL BACKEND

FIELD	DETAIL
Detection Method	Unauthorized privileged transactions appearing on-chain (unexpected mints, pauses, blacklist additions, or deprecation event); transaction monitoring by Tether operations team and external blockchain analytics
Recovery Possible?	Partial
Recovery Authority	Tether Multisig (uncorrupted signers): if compromise is detected before irreversible actions are executed
Recovery Path	Identify and isolate compromised signing infrastructure; rotate affected signer keys via `swapOwner()` with quorum of uncorrupted signers; if needed, execute `transferOwnership()` to move the owner role to a new uncompromised multisig
Prerequisites / Dependencies	Compromise is detected before a `deprecate()` call is executed (deprecation is irreversible); at least 3 uncorrupted signers remain available; Ethereum network operational
Operational Impact	Window between compromise and detection allows unauthorized privileged actions. Mints, pauses, or blacklist changes may have occurred. If deprecation is triggered, impact escalates to Scenario 4.
Residual Risk	High if deprecation is triggered before detection (permanent and irreversible). Medium otherwise: privileges can be restored by key rotation, though any interim unauthorized actions (such as an unauthorized mint) persist on-chain.

Tether's recovery design is centralised but partially resilient at the key-management layer. The 3-of-6 multisig threshold prevents a single key compromise from immediately enabling malicious actions and allows for signer rotation as long as quorum is maintained. However, the design has three structural weaknesses: (1) quorum loss has no recovery path on-chain; (2) the deprecation mechanism is irreversible, so an incorrect `deprecate()` call is a permanent operational failure; and (3) no timelock or advance notice exists for token holders before any privileged action takes effect. Tether has not publicly documented incident response or recovery procedures, so the actual resilience of off-chain coordination under adverse conditions is unknown.

4.5 Multisig Security Analysis

The owner address `0xc6cde7c39eb2f0f0095f41570af89efc2c1ea828` is a Gnosis Safe multisig with a 3-of-6 threshold, as confirmed by Etherscan labeling and independent public sources.

Configuration:

PARAMETER	VALUE
Contract type	Gnosis Safe
Threshold	3-of-6
Individual signer addresses	Not publicly disclosed
Safe version	Not confirmed in available evidence
Modules	Unknown
Guards	Unknown
Fallback handler	Unknown

The 3-of-6 threshold provides meaningful protection against a single compromised key: an attacker who gains control of one or two signer keys cannot execute any privileged transaction unilaterally. This is a material improvement over a bare EOA owner and eliminates single-key compromise as an immediate path to full administrative takeover.

However, the following are unknown and not publicly disclosed: the individual signer addresses and their key management arrangements (HSM, MPC, hardware wallet); whether signers are geographically distributed; whether any signers are shared across other Tether-operated multisigs; and whether any non-standard Gnosis Safe modules, guards, or extensions are enabled. Tether has not published a signer management policy, a key rotation schedule, or information about geographic and institutional diversity of signers. This is a transparency gap that limits the ability to assess the true operational resilience of the multisig independently.

The Gnosis Safe is a well-audited and widely deployed smart contract wallet. No specific vulnerabilities in the Safe contract itself are relevant to this analysis.

5. Part III: Financial Analysis

Financial Risk Rating: Medium | Confidence: Medium

5.1 Underlying Asset Attestation

Tether publishes quarterly reserve attestation reports conducted by BDO, a globally recognized accounting firm. The most recent report assessed here is the Q1 2026 attestation covering the period ending March 31, 2026, published in April 2026 under ISAE 3000 (Revised). This is a limited assurance engagement (negative assurance standard: "nothing has come to our attention"), not a full financial statement audit. BDO does not independently verify every reserve asset with direct custodian confirmations; procedures are agreed with Tether and are less extensive than a statutory audit.

Attestation programme: BDO (ISAE 3000 Revised), quarterly

Most recent attestation report: Q1 2026, March 31, 2026

METRIC	VALUE	SOURCE
Attested reserve assets	$191.77B	BDO ISAE 3000R, March 31, 2026
Attested liabilities (tokens outstanding, all chains)	$183.54B	BDO ISAE 3000R, March 31, 2026
Excess reserve buffer	$8.23B	Derived
Implied collateralization ratio	104.5%	Derived
On-chain token supply (Ethereum, snapshot block 24,941,472)	98.08B USDT	On-chain (`totalSupply()`, block 24,941,472)
Market-reported circulating supply (all chains)	189.59B USDT	CoinGecko, April 24, 2026
Market price	$0.9998	CoinGecko / DeFiLlama, April 24, 2026
24-hour trading volume (CEX, 30 venues)	$36.4B	CoinGecko, April 24, 2026
DEX swap-pool executable liquidity (all chains, pools greater than $100K TVL)	$638M	DeFiLlama, April 24, 2026

Reconciliation: The BDO attestation liabilities ($183.54B, March 31, 2026) are approximately $6.05 billion lower than the market-reported circulating supply ($189.59B, April 24, 2026). This difference is consistent with organic USDT supply growth of approximately $1-2 billion per week in early 2026; the 22-day gap between attestation date and snapshot date plausibly explains the variance and does not indicate a reserve shortfall. A new attestation would be required to confirm reserve coverage as of the exact snapshot date. Ethereum on-chain supply (98.08B USDT) represents approximately 51.7% of market-reported circulating supply; the remaining approximately 91.5B USDT circulates on other chains, principally Tron, BNB Smart Chain, Solana, and Avalanche, and was not independently reconciled on-chain.

5.2 Counterparty Risk Profile

PARTY	ROLE	JURISDICTION	RISK SUMMARY
Tether International, S.A. de C.V.	Issuer	Republic of El Salvador	Dominant stablecoin issuer; privately held; limited public transparency; two prior enforcement actions (CFTC and NY AG, 2021); no public SOC 2; unresolved DOJ investigation; token holders are unsecured creditors
Cantor Fitzgerald & Co. (probable)	Primary T-bill custodian	United States	Identified via press reporting as a probable T-bill custodian; identity not officially disclosed; full extent of asset segregation arrangements unknown
Undisclosed custodians	Gold and Bitcoin custody	Unknown	Identity, jurisdiction, insurance, and segregation arrangements not publicly disclosed for approximately $27B in gold and Bitcoin holdings
BDO	Attestation	International (national member firm)	Accounting firm; ISAE 3000 limited assurance scope; no adverse opinion or resignation risk identified
Major centralized exchanges	Distribution/ liquidity	Multiple	Binance, OKX, Bybit, Kraken, Coinbase, and others; no single exchange creates material counterparty risk at the issuer level

Tether International, S.A. de C.V.: Tether is the dominant stablecoin issuer globally with approximately 60% of total stablecoin supply. Its longevity (operating since 2014) and scale provide meaningful credibility. However, Tether's corporate structure offers limited transparency: it is a privately held entity with no public financial statements beyond the quarterly attestation reports. Ownership and management overlap with Bitfinex (iFinex Inc.), creating concentration risk at the controlling-entity level. Tether's historical track record includes two significant regulatory enforcement actions (CFTC 2021, NY AG 2021, settled in full). While no enforcement actions have occurred since 2021, an unresolved DOJ investigation remains outstanding as of the assessment date. Token holders do not hold a direct legal claim on reserve assets; in an insolvency scenario, USDT holders would rank as unsecured creditors of Tether International S.A. de C.V., not beneficiaries of a ring-fenced trust. This is a material structural risk relative to stablecoin issuers operating under frameworks that mandate client asset segregation.

Cantor Fitzgerald and undisclosed custodians: Tether's primary T-bill custodian relationships are not fully disclosed publicly. Cantor Fitzgerald has been identified via press reporting and Tether's own statements as a significant counterparty for US Treasury bill holdings; other custodians are not named. Gold custodians (approximately $20B) and Bitcoin custodians (approximately $7B) are not publicly identified. The concentration of Tether's reserve assets with a limited number of partially undisclosed custodians creates single-point-of-failure risk. If primary custodians were to freeze assets, fail, or become subject to regulatory action, Tether's ability to honour direct redemptions could be impaired for an extended period. The lack of disclosure makes it impossible to independently assess custodian creditworthiness or the adequacy of asset segregation arrangements.

BDO: BDO is a globally recognized accounting firm. The ISAE 3000 engagement is a standard limited assurance framework; there is no indication of BDO qualification, adverse opinion, or resignation risk. The engagement scope, however, is limited by the procedures agreed with Tether; the attestation does not constitute a full audit. If Tether were to engage a Big Four firm under a full audit standard, confidence in the reserve adequacy assessment would materially increase.

5.3 Liquidity Risks and Scenario Analysis

5.3.1 LIQUIDITY PROFILE

Issuer redemption: Direct redemption from Tether requires a verified Tether account with full KYC/AML. Minimum redemption is $100,000 USD equivalent; the fee is the greater of $1,000 or 0.1% of the redemption amount. Settlement is conducted in business banking days (not 24/7), dependent on banking partners' operating hours. Retail holders cannot directly redeem; they access liquidity exclusively through secondary markets. The direct redemption channel is functionally restricted to institutional participants and cannot process mass-exit volumes.

DEX liquidity: Total reported DEX TVL across all chains for pools above $100K TVL is approximately $5.4 billion. However, the large majority of this TVL is composed of lending and savings protocol deployments (Spark Savings approximately $1.49B, Maple approximately $1.05B, Aave V3, Morpho Blue, Compound V3, and others) that are not immediately executable exit liquidity. Conservative executable DEX swap-pool liquidity is approximately $638 million. Key Ethereum-based DEX pools include Curve DAI-USDC-USDT ($161.7M TVL, $20.9M 24h volume), Uniswap V3 WETH-USDT 0.3% ($81.9M TVL), Fluid USDC-USDT ($46.5M TVL), and Uniswap V3 USDC-USDT 0.01% ($46.1M TVL).

CEX liquidity: Reported 24-hour CEX trading volume across 30 venues is approximately $36.4 billion. This figure represents reported turnover and is not a measure of executable order-book depth. Executable depth at less than 0.5% price impact across major venues (Binance, OKX, Bybit, and comparable tier-1 platforms) is estimated in the range of $1-3 billion, though this cannot be independently confirmed from available data.

USDT is the dominant stablecoin and base trading pair across the global crypto market. This gives it structural liquidity advantages: secondary market buyers (arbitrageurs, market-makers) will step in at small discounts to $1.00, providing a natural liquidity backstop. The peg has remained within approximately plus or minus 0.5% of $1.00 for nearly all of 2023-2026. Historical stress events saw brief discounts of 1-2% before rapid recovery.

VENUE	TYPE	TVL / DEPTH	NOTES
Curve DAI-USDC-USDT (Ethereum)	DEX	$161.7M TVL	$20.9M 24h volume; major stable-swap pool
Uniswap V3 WETH-USDT 0.3% (Ethereum)	DEX	$81.9M TVL	High-frequency ETH/USDT swap pair
Fluid USDC-USDT (Ethereum)	DEX	$46.5M TVL	Lending-integrated stable pool
Uniswap V3 USDC-USDT 0.01% (Ethereum)	DEX	$46.1M TVL	Tight-spread stable pool
Binance (BTC/USDT, USDC/USDT)	CEX	$1B+ estimated order depth	Largest global USDT venue by volume
OKX, Bybit, KuCoin, others	CEX	Substantial but unconfirmed	Combined tier-1 CEX depth estimated $1-3B at less than 0.5% slippage
Spark Savings, Maple, Aave V3, Morpho Blue	Lending protocols	$3.5B+ TVL	Not executable exit liquidity; USDT deployed as lending supply

5.3.2 SCENARIO ANALYSIS

Scenario 1: Base Case

FIELD	DETAIL
Trigger Conditions	Normal operating environment; redemption demand within historical norms; collateral fully attested.
Effect on Collateral	Reserve assets fully attested at 104.5% collateralization; $8.23B excess buffer unchanged. Short-duration T-bills allow partial liquidation via repo at same-day settlement.
Liquidity Runway	Institutional direct redemptions (approximately $500M per day) are processed routinely. Secondary market arbitrage maintains the peg within plus or minus 0.1%. No liquidity constraint under normal conditions.
Anticipated Investor Actions	Institutional redemptions and purchases at prevailing market rates. Secondary market trading at peg. No unusual demand.
Conclusion	No operational concern. The reserve buffer and T-bill liquidity are fully adequate for ordinary redemption demand.
Impact	Low

Scenario 2: Market Stress *(200bp rate shock, Bitcoin and gold price decline, elevated redemption demand)*

FIELD	DETAIL
Trigger Conditions	Broad market stress: a 200bp sudden rate shock causes mark-to-market losses on T-bill holdings; Bitcoin declines 30%; gold declines 10%; redemption demand rises to approximately $10B in 24 hours.
Effect on Collateral	T-bill MTM loss approximately $700M (90-day average duration); Bitcoin decline erases approximately $2.1B; gold correction reduces gold holdings by approximately $2B. Total reserve impairment approximately $4.8B, reducing the excess buffer from $8.23B to approximately $3.4B. The reserve remains solvent.
Liquidity Runway	Elevated demand ($10B/24h) exceeds executable DEX liquidity ($638M) and strains T-bill liquidation timing (T+1 settlement under stress conditions). A redemption queue forms; temporary secondary market peg pressure expected. Residual $3.4B buffer survives simultaneous stress.
Anticipated Investor Actions	Institutional participants queue direct redemptions; retail sellers access secondary markets at a modest discount; arbitrageurs step in as discount widens, providing a partial liquidity offset.
Conclusion	Reserve remains solvent with a compressed but positive buffer. Temporary peg pressure on secondary markets; recovery expected as T-bill liquidation proceeds.
Impact	Medium

Scenario 3: Bank Run *(25% of circulating supply redeemed within 6 hours)*

FIELD	DETAIL
Trigger Conditions	A confidence shock triggers coordinated, rapid redemption of approximately $45.9B (25% of attested liabilities of $183.54B) within 6 hours.
Effect on Collateral	Reserve assets ($191.77B) are intact and solvent; the reserve exceeds liabilities. The risk is a liquidity gate, not insolvency. Assets cannot be liquidated and converted to fiat at the required speed within the 6-hour window.
Liquidity Runway	Executable DEX swap liquidity ($638M) is exhausted within the first 30-60 minutes. Estimated CEX order-book depth ($2-5B at less than 5% slippage) is rapidly consumed. Direct Tether redemption is structurally impossible at this volume in 6 hours given the $100K minimum, KYC requirements, business-hours settlement, and T+1 T-bill settlement.
Anticipated Investor Actions	Panic selling on secondary markets at progressively larger discounts. Institutional arbitrageurs and buyers step in as the discount widens, providing a partial offset but insufficient to prevent material peg dislocation.
Conclusion	Secondary market peg would break materially (estimated 5-15% discount). Reserve solvency is preserved, but significant holders selling at market would experience losses. Recovery contingent on institutional absorption and Tether's ability to resume processing once liquidity gates are lifted.
Impact	High

Scenario 4: Oracle Failure / Price Feed Manipulation

FIELD	DETAIL
Trigger Conditions	Primary USDT price oracle feeds become stale or unavailable for 15 or more minutes; downstream DeFi protocols using USDT as collateral or for pricing are affected.
Effect on Collateral	USDT does not depend on an on-chain oracle for its own peg mechanism or direct redemption process. The redemption price is fixed at $1.00 USD through Tether's off-chain process regardless of oracle availability. Direct solvency and redemption are not affected by oracle failure.
Liquidity Runway	DeFi lending protocols (Aave, Compound, Morpho Blue) that use Chainlink or other feeds for USDT collateral pricing may pause liquidations or use stale prices during the outage, potentially triggering fear-driven secondary market selling (approximately $2B modelled). Available liquidity absorbs this demand with limited peg impact.
Anticipated Investor Actions	DeFi protocol users may face uncertainty around liquidation thresholds; secondary market selling pressure from protocol uncertainty; peg recovers once oracle feeds resume.
Conclusion	Not applicable for direct USDT issuer risk; oracle failure has no impact on Tether's solvency or redemption mechanism. Indirect DeFi ecosystem stress is low to moderate and temporary.
Impact	Low (for USDT directly; Medium for connected DeFi ecosystem)

Scenario 5: Custodian Failure

FIELD	DETAIL
Trigger Conditions	Tether's primary T-bill custodian (believed to include Cantor Fitzgerald) becomes unable to process withdrawals for 48 hours due to insolvency, operational failure, or regulatory seizure.
Effect on Collateral	Reserve assets are not lost in this scenario assuming proper asset segregation; the risk is a temporary operational gate on converting T-bill holdings to fiat. If gold or Bitcoin custodians experience correlated failure, up to approximately $27B in additional reserves could be temporarily inaccessible, but the reserve remains technically solvent.
Liquidity Runway	During the 48-hour window, Tether cannot convert reserve assets to fiat. Available on-chain DEX liquidity ($638M) and estimated CEX order-book depth ($2-5B) are insufficient to absorb large-scale institutional exit demand. Secondary market peg pressure is significant. After 48 hours, if the custodian resumes, Tether can process the accumulated redemption queue.
Anticipated Investor Actions	As custodian distress signals emerge, institutional holders queue redemptions and market makers widen spreads; retail holders face a significant secondary market discount; confidence crisis risk.
Conclusion	Solvency is maintained if asset segregation is adequate (unverifiable from public information). The 48-hour operational gate creates a material confidence crisis and significant secondary market peg pressure. The inability to independently verify custodian segregation quality is the primary reason this scenario carries High impact.
Impact	High

5.4 Regulatory and Legal Jurisdiction

Issuer jurisdiction: Republic of El Salvador

Governing law: El Salvador law (Ley de Servicios de Activos Digitales and CNAD regulatory framework); Terms of Service and Relevant Information Document issued under El Salvador law

REGULATORY ITEM	DETAIL
Primary regulator	Comisión Nacional de Activos Digitales (CNAD), Republic of El Salvador
Licence / registration	Stablecoin Issuer and Digital Assets Service Provider licence under El Salvador's Digital Asset Services Law; also registered as a Money Services Business (MSB) with FinCEN (US) under the Bank Secrecy Act
AML / KYC framework	FinCEN BSA (US): Customer Identification Program, SAR obligations; CNAD (El Salvador): AML requirements under local digital asset law; on-chain blacklisting mechanism as a protocol-level enforcement layer
Enforcement history	CFTC settlement October 2021 ($41M): misleading statements regarding reserve backing between 2016-2019; NY AG settlement February 2021 ($18.5M): false statements regarding reserve backing; both settled in full with no admission of liability; no enforcement actions since 2021
Pending proceedings	DOJ investigation (reported 2023) into potential sanctions evasion and money laundering facilitation; no indictment or charges filed as of May 2026; status remains publicly uncertain

Token holders do not hold a direct legal claim on Tether's reserve assets. USDT represents a contractual right against Tether International S.A. de C.V. to redeem at $1.00 per USDT subject to the Terms of Service (minimum $100K, KYC required, fee payable). In an insolvency scenario, USDT holders would rank as unsecured creditors, not beneficiaries of a segregated trust or SPV. This distinguishes USDT from stablecoins issued under frameworks such as MiCA (EU), which mandate client asset segregation for compliant EMT issuers.

MiCA non-compliance: USDT does not qualify as a MiCA-compliant asset for significant use in the EU. Under MiCA, USD-referenced stablecoins used as a means of exchange qualify as Electronic Money Tokens (EMTs) and require the issuer to be an EU-licensed credit institution or electronic money institution. Tether International S.A. de C.V. is not licensed in any EU Member State. From Q4 2024 through Q1 2025, multiple EU-regulated crypto asset service providers, including Coinbase Europe and Crypto.com EU, delisted or restricted USDT trading pairs. Tether has publicly stated it does not intend to seek MiCA authorisation under the EU framework as currently structured. This creates ongoing structural de-listing pressure in EU-regulated venues.

Tether's 2025 redomiciliation from the British Virgin Islands to El Salvador provides a formal regulatory home (CNAD licence), which is an improvement over the prior BVI regime. However, El Salvador is a small jurisdiction with a nascent regulatory framework and limited international recognition. The effective regulatory oversight of the world's largest stablecoin issuer by a small jurisdiction represents an ongoing structural risk for institutional investors and regulators in major markets. The El Salvador framework does not carry the cross-border enforcement weight of EU, US, or UK regulation. The unresolved DOJ investigation represents the most material near-term regulatory tail risk: a material adverse outcome (indictment, asset freeze, or forced operational shutdown) could materially impair Tether's ability to process redemptions and trigger a systemic confidence crisis.

6. Conclusion

6.1 Composite Risk Rating: Moderate

Composite Confidence: Medium

DOMAIN	RISK RATING	CONFIDENCE
Smart Contract Security	Low	High
Operational Security	Medium	Medium
Financial Integrity	Medium	Medium

The Moderate composite rating reflects the combination of two Medium-rated domains against a Low-rated smart contract domain. USDT's smart contract is well-audited, formally verified, and has operated without incident for over eight years; the two Low-severity findings (SEC-01 and SEC-02) do not create exploitable paths for unauthorized fund extraction. Operational risk is Medium: the 3-of-6 multisig provides meaningful threshold control, but the absence of public disclosure around signer key management, incident response, and monitoring policy prevents the domain from reaching Low. Financial risk is Medium: reserve adequacy is technically strong under the BDO attestation (104.5% collateralization), but the institutionally gated redemption channel, structurally insufficient liquidity runway under a mass-exit scenario, MiCA non-compliance, and an unresolved DOJ investigation are material risk drivers. Composite confidence is Medium: the smart contract evidence base is strong (High confidence), but both Operational and Financial domains are limited by undisclosed off-chain controls and a limited-assurance attestation standard rather than a full audit.

6.2 Improvement Suggestions

- **Operational security transparency:** Tether should publicly disclose its key management policy (HSM/MPC use, key ceremony procedures, and rotation schedules for all Gnosis Safe signers), its recovery and incident response playbook (procedures covering key loss, key compromise, quorum failure, and emergency pause or deprecation scenarios), and its monitoring policy (events and thresholds triggering administrative alerts for minting, burning, pausing, blacklisting, and deprecation activity). None of these are currently publicly available, and this gap materially limits the ability of token holders, custodians, and institutional users to independently assess the operational resilience of the largest stablecoin in the market.
- **Attestation upgrade:** Tether should upgrade the quarterly reserve attestation from ISAE 3000 limited assurance to a full financial statement audit conducted by a Big Four accounting firm. The current limited-assurance standard provides credible but partial assurance; an independent full audit with direct custodian confirmations would materially strengthen reserve transparency and confidence.
- **Custodian disclosure:** Tether should publicly disclose the identity, jurisdiction, regulatory status, and asset segregation arrangements for all material reserve custodians, including those holding T-bill, gold, and Bitcoin reserves. Currently only Cantor Fitzgerald is identified via press reporting. Independent verification of the "solvent but gated" classification in stress scenarios depends on confirming that asset segregation is adequate, which is not possible without custodian identity and structure disclosure.

6.3 Report Validity Timeline

This report is valid as of its publication date. It should be treated as superseded upon any of the following events, whichever occurs first:

- A smart contract upgrade that modifies the in-scope bytecode (including activation of the deprecation mechanism to a new contract address)
- A change to any privileged role holder identified in section 4.1
- A material change to the custodian, redemption model, or reserve composition identified in sections 5.1 and 5.4
- 12 months from the date of publication
