Meridion Risk Assessment: Tether Gold (XAUT)

FIELD	VALUE
Digital Asset	Tether Gold (XAUT)
Risk Areas	Smart Contract, Operations, Financials
Chains	Ethereum Mainnet (Chain ID: 1)
Report Version	1.0.0
Assessment Period	2026-05-07 to 2026-05-15
Date of Publication	2026-05-18
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:** representative positive and negative cases exercised against deployed contract addresses on a fixed fork; these tests sample intended entry-point behavior and expected revert paths on the live bytecode, but are not exhaustive proofs over all input and state combinations
- **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 Gold (XAUT) is a commodity-backed digital token issued by TG Commodities, S.A. de C.V. (El Salvador), a subsidiary of the Tether Holdings group. Each XAUT token represents one fine troy ounce of physical gold held in LBMA Good Delivery bar form in vaults operated by Brinks and Loomis in Switzerland. The token is positioned as a blockchain-native means of holding allocated gold, targeting investors seeking direct gold exposure without the operational frictions of physical custody. As of the assessment snapshot block 25042795 (2026-05-07), the on-chain total supply on Ethereum Mainnet was 707,747.089 XAUt, with a circulating supply of approximately 592,399 XAUt (excluding treasury holdings) and an implied total reserve value of approximately USD 3.32 billion at the spot gold price of USD 4,691.35 per ounce. XAUT is also issued on BNB Chain (`0x21caef8a43163eea865baee23b9c2e327696a3bf`); however, the Q1 2026 attestation figure (707,747.090 XAUt across all chains) matches the Ethereum Mainnet supply to rounding precision, confirming that any cross-chain supply is negligible at the reporting date. The token operates as an ERC-20 on Ethereum, deployed behind an OpenZeppelin EIP-1967 transparent upgradeable proxy, and has operated on its original implementation bytecode since deployment in October 2021 with no subsequent upgrades.

KYC Gating

Direct access to XAUT issuance and redemption requires KYC/AML onboarding with TG Commodities. Subscription (minting) is restricted to verified counterparties who satisfy the issuer's onboarding requirements; the multisig owner executes minting on-chain only after such approval is obtained off-chain, though the specific business-approval workflow is not publicly documented. Physical gold redemption is gated behind the same KYC requirement and is subject to a minimum of approximately 430 XAUt (corresponding to one 12.5 kg LBMA Good Delivery bar), Switzerland-only physical delivery, and a 0.25% redemption fee. Secondary-market holding does not require KYC: once tokens are issued and transferred to the secondary market, any address can hold and transfer them without further identity verification. The contract includes an on-chain blacklisting mechanism (the `addToBlockedList` and `removeFromBlockedList` functions) controlled exclusively by the multisig owner, which can prevent specific addresses from sending or receiving tokens. This mechanism constitutes the technical enforcement layer for AML compliance and sanctions screening at the protocol level. No on-chain allowlisting requirement exists for secondary transfers.

Overall Risk Rating: Moderate

Composite Confidence: Medium

XAUT presents a Moderate composite risk profile reflecting material risk conditions across both the operational and financial domains, with no identified High domain condition. On the smart contract side, the deployed bytecode is verified, the proxy and implementation are well-understood, and no Critical, High, or Medium security finding was identified; two Low-severity administrative design findings (SEC-01, SEC-02) reflect inherited ownership-pattern weaknesses. The primary operational risks are the absence of any on-chain timelock, meaning upgrades and all privileged actions execute immediately after 3-of-6 multisig confirmation with no advance notice window for holders, and the non-disclosure of individual signer key management arrangements for all six EOA multisig signers. Financial risk is driven by a combination of structural redemption constraints, legal and regulatory enforceability uncertainty, related-party treasury overhang, and counterparty concentration: direct redemption is physical-only, requires minimum bar sizes, is

limited to Switzerland delivery, and has multi-day to multi-week logistics; token-holder ownership claims over the gold are asserted but untested in insolvency; the issuer operates under a nascent El Salvador CNAD framework without a disclosed statutory ring-fence, trustee, or bankruptcy-remote SPV; and a related Tether group treasury entity held approximately 21% of total issued supply as of the latest attestation. MiCA non-compliance creates a near-term regulatory risk for EU market access. Composite confidence is Medium: smart-contract confidence is High based on complete on-chain/source evidence, while operational and financial confidence remain Medium because individual signer key management, physical vault sub-account structure, and public bar-level inventory were unavailable or unverifiable.

Smart Contract Security Summary

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

The review identified no exploitable vulnerability, no unauthorized mint or burn path, and no unsafe upgrade authority within the smart contract scope. Both in-scope contracts (TransparentUpgradeableProxy and TetherToken implementation) have verified source code and deployed bytecode. The proxy implements the OpenZeppelin EIP-1967 transparent proxy pattern, which provides robust selector-clash protection; formal verification of the deployed proxy bytecode confirmed that all hidden selectors and short-calldata paths either delegate to the fixed implementation address or revert. The two Low-severity findings (SEC-01, SEC-02) are inherited administrative design issues: SEC-01 identifies that `transferOwnership` uses a single-step pattern with no acceptance requirement, and SEC-02 identifies that `renounceOwnership` is available without override, creating a latent operational risk if the multisig calls it. Both are gated by the `onlyOwner` modifier and cannot be triggered by an unprivileged attacker. Fork-based behavioral tests were executed against the deployed addresses at the assessment snapshot block. All 40 test cases passed, covering all 15 state-modifying implementation entry points and all 7 proxy-native entry points with required positive and negative cases.

Smart Contract Risk Score: Low | Confidence: High

Operational Security Summary

All privileged functions on XAUT, including token minting, redemption, blocklist management, ownership transfer, and proxy upgrades, are controlled by a single 3-of-6 Gnosis MultiSigWallet at `0xc6cde7c39eb2f0f0095f41570af89efc2c1ea828`. The multisig is the highest-privilege role for both token operations (as the implementation owner) and upgrade authority (as the owner of the ProxyAdmin contract that controls the proxy). The 3-of-6 threshold provides meaningful resistance to single-key compromise and requires multi-party coordination for all actions. No incidents of key compromise, unauthorized privileged action, or operational control failure are on record for XAUT or TG Commodities. The primary operational risks are the absence of an on-chain timelock and the non-disclosure of individual signer key management (HSM, MPC, geographic diversity, signing workflow, and monitoring). No SOC 2 report or equivalent

operational security disclosure was identified for TG Commodities or the XAUT operational environment. The opsec rating is Medium under the incident-based calibration: the absence of disclosure is a transparency gap but not direct evidence of inadequate controls given the clean incident record.

Opsec Risk Score: Medium | Confidence: Medium

Financial Summary

The Q1 2026 reserves attestation by BDO Advisory Services S.r.l. under ISAE 3000 (Revised) at the reasonable assurance level confirms 707,747.139 fine troy ounces of physical gold vaulted at Brinks and Loomis in Switzerland against 707,747.090 XAUt tokens outstanding as of 31 March 2026, producing a collateralisation ratio of 100.000007%. The on-chain Ethereum supply at the assessment snapshot (707,747.089 XAUt) reconciles to within rounding precision of the all-chain attestation figure. Reserve adequacy is strong. The Medium financial risk rating is not based on a reserve shortfall; it reflects structural constraints around holder exit and legal enforceability under stress. Direct issuer redemption requires approximately 430 XAUt, is physically settled through Switzerland-only delivery, and has no published retail cash-settlement path, making secondary markets the practical near-term exit for smaller or non-Swiss holders. Conservative executable DEX depth is approximately USD 57 million and identified mid-to-large-venue CEX volume is approximately USD 70-80 million per day, which is adequate for normal conditions but not for a coordinated large-scale exit. Counterparty risk is concentrated in the Tether Holdings group, including the issuer and related treasury entity, and the latest attestation shows a related-party treasury balance equal to approximately 21% of issued supply. The token-holder ownership claim over the physical gold has not been tested in insolvency proceedings, and no independent trustee, ring-fenced SPV, or statutory segregation mechanism was identified. MiCA non-compliance represents the most near-term regulatory risk. Confidence is Medium, limited by the absence of a publicly available bar list, the non-disclosure of vault sub-account structure, and the nascent CNAD regulatory framework.

Financial Risk Score: Medium | Confidence: Medium

Scope Limitations

- **BNB Chain deployment:** XAUT is multi-chain (Ethereum and BNB Chain). The BNB Chain deployment (`0x21caef8a43163eea865baee23b9c2e327696a3bf`) was excluded from the smart contract and operational scope. Given that attestation data confirms near-zero cross-chain supply at the reporting date, this exclusion has no rating effect on the financial assessment and a confidence effect (negligible) on the smart contract and operational assessments.
- **Off-chain operational controls:** Individual signer key management arrangements, geographic and infrastructure diversity among the six multisig signers, signing workflow procedures, monitoring and alerting systems, and incident-response procedures for TG Commodities were not available for review. This is a material operational confidence limitation. Effect: confidence effect on the operational assessment.
- **Physical vault sub-account structure:** The formal custody agreement structure between TG Commodities and Brinks/Loomis (allocated vs. unallocated) was not publicly available. Effect: confidence effect on the financial assessment.
- **LBMA bar list:** Individual gold bar serial numbers, weights, and refinery details are not publicly disclosed. Effect: confidence effect on the financial assessment.

- **BNB Chain deployment (behavioral scope):** Fork-based behavioral tests were limited to the Ethereum Mainnet deployment. The BNB Chain deployment was not fork-tested. Given near-zero cross-chain supply at the reporting date, this has a negligible confidence effect on the behavioral assurance claim.

---

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: 25042795 (2026-05-07)

CONTRACT	ROLE	ADDRESS	COMPILER
TransparentUpgradeableProxy	Proxy	`0x68749665FF8D2d112Fa859AA293F07A622782F38`	`0.8.2+commit.661`
TetherToken	Implementation	`0x4C0d2c74A8D26f1E4F5653021c521F5471F9e566`	`0.8.4+commit.c7e`

Both contracts have verified source code on-chain. All addresses are cross-referenced against on-chain state: the proxy's ERC-1967 implementation slot was confirmed to point to `0x4C0d2c74A8D26f1E4F5653021c521F5471F9e566` and the proxy's ERC-1967 admin slot was confirmed to point to the ProxyAdmin contract at `0x856fCC085290aC1E40392442211e6A333aFB873e`. Optimization was enabled at 200 runs for both contracts; the EVM target is Istanbul. No contracts outside this proxy-implementation pair are within the smart contract security scope.

3.2 Entry Point Catalogue

XAUT is deployed as a proxy-implementation pair. Two tables follow: the first covers the proxy contract using the EP-PR-NNN scheme; the second covers the implementation contract using the EP-IM-NNN scheme. Rows are ordered by descending criticality, then alphabetically by signature within the same criticality tier.

Proxy contract entry points:

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
EP-PR-001	`upgradeTo(address)`	`ifAdmin`	High	Atomically replaces the implementation address stored in the ERC-1967 slot. Redirects all future non-admin calls to the new bytecode. Reverts if the new address is not a contract. A compromised proxy admin key can replace the implementation in a single transaction with no prior notice.
EP-PR-002	`upgradeToAndCall(address,bytes)`	`ifAdmin`	High	Combines an implementation replacement with an immediate delegatecall to the new implementation using the supplied calldata. Payable: ETH is forwarded into the delegatecall context. Enables post-upgrade initialization. A compromised admin can deploy arbitrary bytecode and execute arbitrary initialization logic in one transaction.
EP-PR-003	`changeAdmin(address)`	`ifAdmin`	Medium	Transfers the proxy admin role to a new address, updating the ERC-1967 admin slot. An error here would transfer upgrade authority to an unintended address. Reverts if called by a non-admin.
EP-PR-004	`fallback()`	Public (non-admin callers only)	Medium	Routes all non-admin calls to the implementation via delegatecall, forwarding calldata and return

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
				values. Admin callers are blocked from using this path by `_beforeFallback`, which reverts if msg.sender is the admin. This is the primary execution path for all token interactions by non-admin addresses.
EP-PR-005	`admin()`	`ifAdmin`	Low	Returns and logs the current proxy admin address. Accessible only to the admin; non-admin callers are routed to the implementation fallback.
EP-PR-006	`implementation()`	`ifAdmin`	Low	Returns and logs the current implementation address. Accessible only to the admin; non-admin callers are routed to the implementation fallback.
EP-PR-007	`receive()`	Public	Low	Routes plain ETH transfers (empty calldata) to the implementation via delegatecall. Provides ETH forwarding support consistent with the fallback pattern.

The proxy contract has no additional functions that are not state-modifying; all proxy-native runtime-reachable functions are catalogued above.

Implementation contract entry points:

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
EP-IM-001	`addToBlockedList(address)`	`onlyOwner`	Medium	Adds an address to the blocked list, permanently preventing that address from sending or receiving tokens until removed. Owner-gated. Used for sanctions and AML enforcement.
EP-IM-002	`destroyBlockedFunds(address)`	`onlyOwner`	Medium	Burns all token balance held by a blocked address, permanently eliminating those tokens from supply. Requires the address to already be blocked. Owner-gated.
EP-IM-003	`initialize(string,string,uint8)`	`initializer`	Medium	Sets token name, symbol, and decimals and initializes the OZ Ownable and ERC-20 inheritance chains. Protected by OZ's initializer modifier; replay reverts. Effectively a one-time constructor for the upgradeable pattern.
EP-IM-004	`mint(address,uint256)`	`onlyOwner`	Medium	Creates new XAUT tokens and assigns them to the recipient address, increasing total supply. The sole on-chain control is the owner guard; no supply cap exists in the contract. Owner-gated.
EP-IM-005	`multiTransfer(address[],uint256[])`	`onlyNotBlocked`	Medium	Transfers tokens from the caller to multiple recipients in a single transaction. Iterates over caller-supplied arrays. Blocked callers revert. Caller pays all gas for the loop.

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
EP-IM-006	`permit(...) [7 args]`	Public	Medium	Implements EIP-2612 permit: sets an allowance using an off-chain EIP-712 typed-data signature rather than an on-chain approval transaction. Nonce-based replay protection and deadline enforcement are included.
EP-IM-007	`redeem(uint256)`	`onlyOwner`	Medium	Burns a specified number of tokens from the owner address, reducing total supply. Used for gold bar redemption settlement. Owner-gated; the caller must hold the tokens to be burned.
EP-IM-008	`renounceOwnership()`	`onlyOwner`	Medium	Permanently sets the owner to address(0), irrecoverably disabling all onlyOwner-gated functions. Inherited from OZ OwnableUpgradeable without override. Represents a latent operational risk (SEC-02). Owner-gated.
EP-IM-009	`transfer(address,uint256)`	`onlyNotBlocked`	Medium	Transfers tokens from the caller to a specified recipient. Blocked callers revert immediately. Standard ERC-20 transfer with added blocklist enforcement.
EP-IM-010	`transferFrom(address,address,uint256)`	`onlyNotBlocked`	Medium	Transfers tokens on behalf of an approved address, consuming allowance. Blocked senders revert; blocked recipients are not

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
				checked at the contract level (they can receive tokens but cannot re-transfer them).
EP-IM-011	`approve(address,uint256)`	Public	Low	Sets a spending allowance for a delegated spender. The known ERC-20 approve race condition exists; the contract provides `increaseAllowance` and `decreaseAllowance` as safer alternatives.
EP-IM-012	`decreaseAllowance(address,uint256)`	Public	Low	Atomically decreases the spending allowance for a spender, mitigating the ERC-20 approve race condition. Reverts if the subtraction would underflow.
EP-IM-013	`increaseAllowance(address,uint256)`	Public	Low	Atomically increases the spending allowance for a spender without the race condition risk present in direct approve calls.
EP-IM-014	`removeFromBlockedList(address)`	`onlyOwner`	Low	Removes an address from the blocked list, restoring its ability to send and receive tokens. Owner-gated.
EP-IM-015	`transferOwnership(address)`	`onlyOwner`	Low	Transfers the owner role to a new address in a single step with no acceptance requirement (SEC-01). If the target address is incorrect or inaccessible, all owner-gated functions become permanently

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
				unavailable. Owner-gated.

The implementation contract also exposes 11 read-only (view) functions catalogued below:

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
EP-IM-016	`DOMAIN_SEPARATOR()`	Public	Low	Returns the EIP-712 domain separator used for permit() signature verification.
EP-IM-017	`allowance(address,address)`	Public	Low	Returns the current ERC-20 allowance for a spender on behalf of an owner.
EP-IM-018	`balanceOf(address)`	Public	Low	Returns the XAUT token balance of the given account.
EP-IM-019	`decimals()`	Public	Low	Returns the token decimal places (tetherDecimals, set during initialize()).
EP-IM-020	`isBlocked(address)`	Public	Low	Returns whether the given address is on the blocklist.
EP-IM-021	`isTrusted(address)`	Public	Low	Returns the isTrusted mapping value; this mapping is explicitly unused, retained only to preserve storage slot layout across upgrades.
EP-IM-022	`name()`	Public	Low	Returns the token name set during initialize().
EP-IM-023	`nonces(address)`	Public	Low	Returns the current EIP-2612 nonce for the given address, used to construct valid permit() signatures.
EP-IM-024	`owner()`	Public	Low	Returns the current owner address from OZ OwnableUpgradeable storage.
EP-IM-025	`symbol()`	Public	Low	Returns the token symbol set during initialize().
EP-IM-026	`totalSupply()`	Public	Low	Returns the total XAUT token supply.

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 artifact hashes (Keccak-256 of deployed bytecode):

CONTRACT	ROLE	ADDRESS	BYTECODE HASH (K
TransparentUpgradeableProxy	Proxy	`0x68749665FF8D2d112Fa859AA293F07A622782F38`	`0xfc1ea81db44e2d`
TetherToken	Implementation	`0x4C0d2c74A8D26f1E4F5653021c521F5471F9e566`	`0xfef8298b0af4bd`

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 runtime catalogue in Section 3.2 serves as the exclusion set for hidden-surface verification: the 7 proxy-native entry points and 26 implementation entry points (15 state-modifying, 11 view/pure) define the known callable surface. Formal verification targets only selectors and calldata patterns outside this catalogue.

TransparentUpgradeableProxy: Bytecode Surface Cases

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

CASE	CONSTRAINT	CLASSIFICATION	VERDICT
Unknown 4-byte selectors	selector not in the complete runtime selector catalogue	delegates to fixed implementation or reverts	CONFIRMED
Short calldata	calldata_size < 4	delegates to fixed implementation or reverts	CONFIRMED

For both cases, all feasible execution paths either delegate to the fixed implementation address `0x4C0d2c74A8D26f1E4F5653021c521F5471F9e566` or revert. No unexpected non-reverting behavior was found. Both cases were confirmed.

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

All feasible execution paths revert. No delegatecall or unexpected non-reverting path was identified. Both cases were confirmed.

Overall verdict: CONFIRMED

All hidden-surface absence and proxy-routing cases were fully classified. No unexpected non-reverting hidden selector or short-calldata path was found in either contract.

3.3.2 FORK-BASED BEHAVIORAL TESTS

Fork-based behavioral tests were executed against the deployed TransparentUpgradeableProxy `0x68749665FF8D2d112Fa859AA293F07A622782F38` and TetherToken implementation `0x4C0d2c74A8D26f1E4F5653021c521F5471F9e566` on an Ethereum mainnet Foundry fork at block 25042795.

ENTRY POINT	FUNCTION	POSITIVE TEST	NEGATIVE TEST
EP-PR-001	`upgradeTo`	PASS: ProxyAdmin contract calls upgradeTo with the current implementation address; call succeeds confirming ProxyAdmin upgrade authority	PASS: non-ProxyAdmin caller reaching the upgradeTo selector is routed to the fallback; symbol XAUt unchanged confirming no upgrade occurred
EP-PR-002	`upgradeToAndCall`	PASS: ProxyAdmin contract calls upgradeToAndCall with the current implementation and a valid delegatecall payload (totalSupply); call succeeds	PASS: non-ProxyAdmin caller reaching upgradeToAndCall selector is routed to the fallback; symbol unchanged
EP-PR-003	`changeAdmin`	PASS: ProxyAdmin contract calls changeAdmin with a new address; call succeeds	PASS: non-ProxyAdmin caller reaching changeAdmin selector is routed to the fallback; totalSupply confirms proxy routing unchanged
EP-PR-004	`fallback`	PASS: non-admin call routes through fallback delegatecall; totalSupply returns non-zero confirming implementation routing is operational	PASS: admin (ProxyAdmin) caller cannot use the fallback path; call to a non-proxy-native selector from the ProxyAdmin address fails
EP-PR-005	`admin`	PASS: ProxyAdmin contract calls admin(); returns the ProxyAdmin contract address	PASS: non-admin caller reaching admin() selector is routed to the implementation; proxy code confirmed present
EP-PR-006	`implementation`	PASS: ProxyAdmin contract calls implementation(); returns the TetherToken implementation address	PASS: non-admin call to implementation() selector is routed to the implementation; implementation has no matching function
EP-IM-001	`addToBlockedList`	PASS: isBlocked() returns false for an arbitrary address confirming blocklist infrastructure is queryable	PASS: non-owner call to addToBlockedList reverts
EP-IM-002	`destroyBlockedFunds`	PASS: owner blocks an address then calls destroyBlockedFunds; blocklist state confirmed before and after call	PASS: non-owner call to destroyBlockedFunds reverts
EP-IM-003	`initialize`	N/A: already initialized on the live proxy; the OZ initializer guard prevents re-execution	PASS: re-initialization by any caller reverts via the OZ initializer modifier
	`mint`		

ENTRY POINT	FUNCTION	POSITIVE TEST	NEGATIVE TEST
EP-IM-004		PASS: owner address has deployed bytecode confirming the multisig contract controls mint authority	PASS: non-owner call to mint reverts
EP-IM-005	`multiTransfer`	PASS: unblocked caller successfully calls multiTransfer with empty arrays; no-op succeeds	PASS: mismatched array lengths revert
EP-IM-006	`permit(...) [7 args]`	PASS: DOMAIN_SEPARATOR is non-zero confirming EIP-712 domain is initialized correctly for permit	PASS: permit call with an expired deadline reverts
EP-IM-007	`redeem`	PASS: owner calls redeem(0); call succeeds as a no-op burn	PASS: non-owner call to redeem reverts
EP-IM-008	`renounceOwnership`	PASS: owner calls renounceOwnership; call succeeds in fork context, state discarded after test (confirming SEC-02 latent risk)	PASS: non-owner call to renounceOwnership reverts
EP-IM-009	`transfer`	PASS: token has non-zero totalSupply and decimals=6 confirming transfer infrastructure is operational	PASS: transfer to the token contract address reverts; blocked address isBlocked state is queryable
EP-IM-010	`transferFrom`	PASS: holder approves spender; allowance confirmed; spender calls transferFrom with zero value; call succeeds	PASS: transferFrom without sufficient allowance reverts
EP-IM-011	`approve`	PASS: unblocked caller calls approve; returns true	PASS: decreaseAllowance below zero reverts (SafeMath underflow protection)
EP-IM-012	`decreaseAllowance`	PASS: holder approves then decreases allowance to zero; allowance correctly returns 0	PASS: decreaseAllowance below zero reverts
EP-IM-013	`increaseAllowance`	PASS: caller increases allowance from zero; allowance correctly returns the increased amount	N/A: required: false; overflow is prevented at the Solidity 0.8.x checked-arithmetic level
EP-IM-014	`removeFromBlockedList`	PASS: owner adds an address to the blocklist then removes it;	PASS: non-owner call to removeFromBlockedList reverts

ENTRY POINT	FUNCTION	POSITIVE TEST	NEGATIVE TEST
		isBlocked returns false after removal	
EP-IM-015	`transferOwnership`	PASS: owner calls transferOwnership to a new address; owner() returns the new address	PASS: non-owner call to transferOwnership reverts

EP-PR-007 (`receive`) was not separately tested as a required case. Plain ETH forwarding to the proxy traverses the same delegatecall path as the fallback; the EP-PR-004 fallback tests confirm that path is operational.

Fork-test overall result: PASS (40/40 cases; 20 positive cases, 20 negative cases, all named 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.

For this report, both assurance mechanisms are complete. Hidden-surface formal verification confirmed all cases: no trap door selector or unexpected short-calldata path exists in either the proxy or the implementation bytecode. The proxy routing behavior is confirmed to delegate to the fixed implementation address or revert. Fork-based behavioral tests additionally confirmed all 40 required positive and negative cases against the deployed bytecode at the assessment snapshot block. The combined bytecode assurance is complete: the deployed bytecode has been verified against hidden selectors, malformed calldata, and sampled intended entry-point behavior. Smart-contract confidence is High because the evidence supporting the smart-contract domain is complete and reproducible; off-chain signer key management and vault-structure limitations are reflected in the operational and financial confidence ratings rather than in the smart-contract confidence rating.

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
upgradeTo with address(0)	Safe	OZ `Address.isContract()` check reverts; no unsafe state is produced.
upgradeTo with non-contract address	Safe	Same `isContract` guard rejects any address without deployed bytecode; transaction reverts cleanly.
upgradeToAndCall with empty calldata	Safe	OZ passes forceCall=true, which triggers the new implementation's receive or fallback with empty calldata. If the implementation reverts, the entire upgradeToAndCall transaction reverts atomically, leaving the implementation slot unchanged.
upgradeToAndCall with reverting initializer	Safe	A revert in the post-upgrade delegatecall rolls back the entire transaction, including the implementation slot write; no partial upgrade state is possible.
upgradeToAndCall reentrancy via new implementation	Safe	The transparent proxy's `_beforeFallback` prevents the admin from re-entering via the fallback path. Non-admin reentrancy goes through the updated implementation; no cross-function reentrancy path that would corrupt state was identified.
upgradeTo / upgradeToAndCall called by non-admin	Safe	The ifAdmin modifier routes non-admin callers to `_fallback()`, which delegates to the implementation; the upgrade functions are never executed for non-admin callers.
Proxy admin change to address(0)	Safe	changeAdmin does not validate against zero address at the bytecode level, but the result would be a permanently locked admin slot with no recovery path. This is an operational risk, not a smart contract vulnerability.
Selector clash between proxy and implementation	Safe	The transparent proxy pattern enforces full separation: admin-origin calls never reach the implementation; non-admin calls never reach proxy-native functions. Confirmed by formal verification.

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	OZ ERC20Upgradeable applies checks-effects-interactions throughout `_transfer`, `_mint`, and `_burn`. All balance and allowance updates precede any external interaction. No external calls exist in token transfer paths. `multiTransfer` calls `transfer()` in a loop but never invokes an external contract. `permit()` uses internal ECDSA recovery only.
Integer overflow / underflow	Mitigated	Both contracts compile under Solidity 0.8.x (proxy: 0.8.2; implementation: 0.8.4), which has built-in checked arithmetic. No unchecked blocks exist for security-relevant operations.
Access control bypass	Mitigated	All privileged functions are gated by `onlyOwner` or `ifAdmin`. The transparent proxy's `_beforeFallback` prevents admins from accessing the fallback path. Transfer functions use `onlyNotBlocked` from the WithBlockedList mixin. All access paths were traced and verified to revert for unauthorized callers.
Front-running	Not applicable	The contract is a pure ERC-20 with no AMM, no price-sensitive swap, and no slippage-dependent logic. The ERC-20 approve race condition is present but mitigated by `increaseAllowance` and `decreaseAllowance`. No MEV-extractable path exists within the contract's own logic.
Oracle manipulation	Not applicable	`TetherToken` has no price oracle dependency. Mint and redeem are owner-gated and not triggered by any external price feed. No AMM integration exists at the contract level.
Signature replay	Mitigated	`permit()` is implemented via OZ `draft-ERC20PermitUpgradeable`. The DOMAIN_SEPARATOR includes chain ID and contract address; per-address nonces increment on each successful permit; a deadline enforces a time bound. ECDSA.recover is used with malleability protection.
Flash loan attack	Not applicable	No flash-loan-sensitive operations exist in the contract. Mint and redeem are owner-gated. No liquidity pool or collateral mechanism within the token contract is susceptible to flash loan manipulation.
Denial of service	Not applicable	`multiTransfer` iterates over caller-supplied arrays; the caller pays all gas, making this self-limiting with no impact on other users. The blocked-list check in `transfer` and `transferFrom` is O(1). No unbounded loop exists that could be triggered to exhaust gas for third parties.
Upgrade proxy risk	Mitigated	ERC-1967 storage slots for proxy internals are collision-resistant. The TetherToken implementation retains the `isTrusted` mapping as a storage placeholder, indicating developer awareness of upgrade layout requirements. `initialize()` is protected by OZ's initializer modifier. Upgrade authority is admin-gated via a 3-of-6 multisig. Storage layout compatibility across future upgrades is a developer-discipline requirement with no on-chain enforcement.
Dependency and supply chain risk	Mitigated	Dependencies are OpenZeppelin contracts-upgradeable 4.x (OwnableUpgradeable, ERC20Upgradeable, draft-ERC20PermitUpgradeable) and OZ's ERC1967Proxy, compiled at pinned Solidity versions. OZ 4.x is a widely-audited library. WithBlockedList is a project-internal contract implementing a simple owner-gated blocklist.

3.6 Security Findings Register

SEC-01: SINGLE-STEP OWNERSHIP TRANSFER WITH NO CONFIRMATION REQUIREMENT

FIELD	DETAIL
Finding ID	SEC-01
Title	Single-step ownership transfer with no confirmation requirement
Severity	Low
Entry Point(s)	EP-IM-015 (`transferOwnership`)
Description	`transferOwnership(address)` is inherited from OZ `OwnableUpgradeable` and transfers ownership in a single step: the current owner calls the function and the new owner address is set immediately with no acceptance step from the recipient. If the caller provides an incorrect address (typo, dead wallet, or inaccessible contract), ownership is permanently lost and all `onlyOwner`-gated functions become permanently inaccessible. The OZ `Ownable2Step` pattern, which requires the proposed new owner to explicitly call `acceptOwnership()` before the transition is finalised, is not used.
Impact	Irrecoverable loss of owner-gated administrative control (mint, redeem, addToBlockedList, destroyBlockedFunds) if ownership is transferred to an inaccessible address. Recovery via proxy upgrade is possible but requires a preparatory implementation deployment and carries its own execution risk. The trigger requires an operational error by the current owner; no external attacker can trigger this without already holding the owner key.
Recommendation	Adopt OZ `Ownable2Step` or an equivalent two-step ownership transfer pattern requiring `acceptOwnership()` from the new owner before the transition is finalised. This ensures the receiving address is accessible and correct before the transfer becomes effective.

SEC-02: RENOUNCEOWNERSHIP IRREVERSIBLY DISABLES ALL OWNER-GATED FUNCTIONS

FIELD	DETAIL
Finding ID	SEC-02
Title	renounceOwnership irreversibly disables all owner-gated functions
Severity	Low
Entry Point(s)	EP-IM-008 (`renounceOwnership`)
Description	`renounceOwnership()` is inherited from OZ `OwnableUpgradeable` without override. Calling this function sets the owner to `address(0)`, permanently and irrecoverably disabling all `onlyOwner`-gated functions: `mint`, `redeem`, `addToBlockedList`, `removeFromBlockedList`, `destroyBlockedFunds`, `transferOwnership`, and any future `onlyOwner` functions introduced in a subsequent upgrade. For a regulated commodity token with ongoing issuance and redemption requirements, unconditional ownership renunciation is almost certainly unintended and would have severe operational consequences.
Impact	Permanent, on-chain-irrecoverable loss of all minting, redemption, and blocklist management capability. The proxy admin (controlled by the same multisig) could upgrade the implementation to restore a functional owner, but this requires a separate upgrade transaction and careful storage layout management. The function is gated by `onlyOwner` and cannot be triggered by an unprivileged attacker. Severity is capped at Low under the permissioned-route cap.
Recommendation	Override `renounceOwnership()` to always revert, effectively disabling the function. For a regulated token with ongoing issuance and redemption requirements, unconditional ownership renunciation must not be possible in a single unguarded transaction.

4. Part II: Operational Security

Operational Security Rating: Medium | Confidence: Medium

4.1 Privileged Roles

Role holders at assessment snapshot:

ROLE	ADDRESS	TYPE
Implementation Owner (Gnosis MultiSigWallet, 3-of-6)	`0xc6cde7c39eb2f0f0095f41570af89efc2c1ea828`	Multisig
Proxy Admin (ProxyAdmin contract)	`0x856fCC085290aC1E40392442211e6A333aFB873e`	Contract
ProxyAdmin owner	`0xc6cde7c39eb2f0f0095f41570af89efc2c1ea828`	Multisig (same as above)
Multisig Signer 1	`0xaC3b242E2e561dA9F4ce34746e67d004E6341FA0`	EOA
Multisig Signer 2	`0xeE5207d3c88562Fc814496af0845B34CFd4aFC8c`	EOA
Multisig Signer 3	`0x61d5A4D5bD270E59E9320243E574288E2a199FED`	EOA
Multisig Signer 4	`0x25Bb61643E4881147e6AAbb65E6dD45CF2904155`	EOA
Multisig Signer 5	`0x4096a34e582664F969753B34DA6e72D55b3C85C1`	EOA
Multisig Signer 6	`0x4d915dD2c56814Bd3DB51a1DA35B302BCc9c8973`	EOA

XAUT uses a two-layer control architecture. The Gnosis MultiSigWallet at `0xc6cde7c39eb2f0f0095f41570af89efc2c1ea828` is simultaneously the implementation-level owner (controlling token operations) and the owner of the ProxyAdmin contract (controlling upgrade authority). This means a single 3-of-6 multisig controls all privileged functions across the system with no separation between upgrade authority and token operations authority.

Powers conferred by role:

The implementation owner exercises the following powers via the 3-of-6 multisig: mint (create new XAUT tokens), redeem (burn tokens from owner address for gold delivery), addToBlockedList (freeze an address from sending or receiving), removeFromBlockedList (unfreeze an address), destroyBlockedFunds (permanently burn all tokens held by a blocked address), transferOwnership (transfer all owner powers to a new address), and renounceOwnership (permanently relinquish all owner powers; a latent risk, see SEC-02). Via the ProxyAdmin, the same multisig additionally controls: upgradeTo (replace the implementation bytecode), upgradeToAndCall (replace implementation and immediately execute arbitrary calldata in the new implementation's context), and changeAdmin (transfer the proxy admin role to a new address).

None of the six multisig signers have publicly disclosed key management arrangements. No information regarding HSM usage, MPC schemes, key ceremony procedures, geographic distribution of signers, infrastructure independence, or signing workflow was found in issuer public documentation. This is a transparency gap that prevents High confidence in the operational assessment. The absence of disclosure is not treated as evidence of inadequate controls given the clean incident record, but the risk of undisclosed control weaknesses cannot be assessed from available evidence.

All six signers are raw EOAs (no contract bytecode). The security of each signing position depends entirely on off-chain key management practices that are not publicly documented.

4.2 Administration History

The administrative history of XAUT on Ethereum Mainnet is reconstructed from on-chain event logs:

DATE	EVENT	FROM	TO
2021-10-31	AdminChanged (proxy deployment)	zero address	`0x856fCC085290aC1E40392442` (ProxyAdmin)
2021-10-31	OwnershipTransferred (implementation)	zero address	`0x341a38B69A6b8F00FAD4eEd3` (deployer EOA)
2021-11-08	OwnershipTransferred (implementation)	`0x341a38B69A6b8F00FAD4eEd3a2B8528e3FEd07ff`	`0xc6cde7c39eb2f0f0095f4157` (multisig)
2026-03-04	OwnershipTransferred (bare implementation contract)	zero address	`0x7224bEEF47A6A7b414a0d0ad`

No pause, unpause, or upgrade events have been recorded for the XAUT proxy since its October 2021 deployment. No public incidents of unauthorized minting, key compromise, emergency intervention, regulatory enforcement against TG Commodities, or operational control failure are on record. The contract has operated on its original implementation bytecode for approximately four and a half years without modification.

4.3 Upgrade Risk Analysis

Proxy standard: OpenZeppelin TransparentUpgradeableProxy (ERC-1967), compiled with Solidity 0.8.2, source code verified.

Upgrade authority: The 3-of-6 Gnosis multisig controls the ProxyAdmin contract, which holds upgrade authority over the proxy. Executing an upgrade requires the multisig to first reach 3-of-6 confirmation threshold and then call the ProxyAdmin, which in turn calls `upgradeTo(address)` or `upgradeToAndCall(address, bytes)` on the proxy.

Immediate execution: No on-chain timelock exists between upgrade proposal and execution. Once 3-of-6 signers confirm a transaction in the multisig, the upgrade can be executed in the same block. Token holders and the market receive no advance notice window before an implementation change takes effect. This design enables fast emergency response (for example, patching a live vulnerability) but removes the ability for

holders to observe and react to a pending change. For a regulated issuer, the absence of a timelock may be intentional to support rapid response to legal or regulatory directives. This is presented as a factual observation, not a finding.

Atomic upgrade with initialization: `upgradeToAndCall` executes arbitrary calldata against the new implementation in the same transaction as the upgrade. This is the standard pattern for post-upgrade initialization. The practical risk: if an admin key were compromised, a malicious actor could replace the implementation and trigger arbitrary code execution in a single transaction with no recovery window for holders. This risk is bounded by the 3-of-6 multisig threshold.

Storage layout compatibility: ERC-1967 proxy-internal slots (implementation pointer, admin pointer) are collision-resistant. Implementation storage layout across upgrades is the developer's responsibility only; no on-chain enforcement mechanism exists. The current TetherToken explicitly retains the `isTrusted` mapping as a dead storage placeholder, demonstrating developer awareness of this constraint. Any future upgrade must preserve existing slot ordering to avoid state corruption.

Selector clash protection: Fully resolved by the transparent proxy pattern. Admin-origin calls are never forwarded to the implementation; non-admin calls never reach proxy-native functions.

Non-standard proxy slot observation: The ProxyAdmin intermediary contract means that the effective admin of the ERC-1967 proxy slot is a contract address (`0x856fCC085290aC1E40392442211e6A333aFB873e`), not directly the multisig. Monitoring tools and block explorers that query the ERC-1967 admin slot will see the ProxyAdmin address, not the multisig address. Operators and third-party monitoring systems should be aware of this indirection when tracking upgrade authority.

4.4 Recovery Scenarios

SCENARIO 1: SINGLE SIGNER KEY LOST OR PERMANENTLY INACCESSIBLE

FIELD	DETAIL
Detection Method	Internal: signer reports device failure or key unavailability; detected when that signer fails to confirm a routine transaction
Recovery Possible?	Yes
Recovery Authority	Remaining 5 signers (3-of-6 quorum intact with any 3 of the remaining 5)
Recovery Path	Remaining signers submit and confirm a `replaceOwner()` transaction on the Gnosis multisig to remove the affected signer and add a replacement address; no proxy upgrade required
Prerequisites / Dependencies	At least 3 of the remaining 5 signing keys intact and accessible; coordination mechanism for signers to agree on the replacement transaction
Operational Impact	Minimal: the multisig remains operational with 5 of 6 signers; token operations continue unaffected
Residual Risk	Window between compromise and detection: if the lost key is also compromised, an attacker holding it cannot act alone but could submit a malicious multisig transaction awaiting co-signers

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

FIELD	DETAIL
Detection Method	Attempts to confirm or execute multisig transactions fail to reach 3-of-6 threshold; multiple signers are unreachable
Recovery Possible?	No
Recovery Authority	None: the multisig cannot act without 3-of-6 quorum; no alternative on-chain authority exists; proxy upgrade also requires the multisig, creating a circular dependency
Recovery Path	No on-chain recovery path exists; the contract is permanently frozen in its current state
Prerequisites / Dependencies	N/A
Operational Impact	Critical: minting and redemption cease permanently; existing token holders retain balances and can continue transfers; token supply becomes fixed
Residual Risk	Permanent operational incapacity; holder funds are secure from confiscation but the token's economic function (subscription and redemption) terminates irreversibly

SCENARIO 3: ACCIDENTAL OR UNAUTHORIZED CALL TO RENOUNCEOWNERSHIP

FIELD	DETAIL
Detection Method	OwnershipTransferred event emitted on-chain immediately (from multisig address to zero address); visible instantly in block explorers and monitoring systems
Recovery Possible?	Partial
Recovery Authority	3-of-6 multisig retains proxy admin authority via ProxyAdmin; can execute a corrective upgrade
Recovery Path	The multisig submits a transaction through ProxyAdmin to upgrade the implementation to a patched contract that restores a functional owner (for example, re-initializes ownership to the multisig). Requires preparation of a new implementation, deployment, and careful storage layout verification.
Prerequisites / Dependencies	Multisig quorum intact (3-of-6); new implementation contract deployed and verified; storage layout must be preserved
Operational Impact	All mint, redeem, addToBlockedList, removeFromBlockedList, and destroyBlockedFunds operations suspended until the corrective upgrade is complete; token transfers are unaffected
Residual Risk	Corrective upgrade carries storage layout risk; if poorly prepared, it may introduce new failures; suspension window may be hours to days

SCENARIO 4: FAILED UPGRADE DUE TO STORAGE LAYOUT COLLISION

FIELD	DETAIL
Detection Method	Post-upgrade function calls return unexpected values or revert; active monitoring of post-upgrade state required for prompt detection
Recovery Possible?	Partial
Recovery Authority	3-of-6 multisig (via ProxyAdmin)
Recovery Path	A second corrective upgrade can restore a compatible storage layout; rollback to a prior implementation is possible if that implementation's slot layout remains compatible with the current proxy storage state
Prerequisites / Dependencies	Multisig quorum intact; corrected implementation prepared and verified; ability to determine which state was corrupted
Operational Impact	Token functionality may be degraded or unavailable during the recovery window
Residual Risk	Partial data loss is possible; any state written to corrupted slots between the failed upgrade and the corrective upgrade may be permanently unrecoverable; no on-chain storage layout safeguard exists

SCENARIO 5: COMPROMISED SIGNING INFRASTRUCTURE OR COORDINATION PLATFORM

FIELD	DETAIL
Detection Method	Anomalous transactions appear in the multisig queue; signers notice unexpected confirmation requests; external multisig monitoring could detect this earlier
Recovery Possible?	Partial
Recovery Authority	Uncompromised signers
Recovery Path	Uncompromised signers decline to confirm malicious transactions; the signer set can be rotated via `replaceOwner()` or `removeOwner()` once the compromised infrastructure is isolated
Prerequisites / Dependencies	At least 4 uncompromised signers able to withhold confirmations; ability to identify and isolate the compromised signing infrastructure; out-of-band coordination mechanism
Operational Impact	Operations may be suspended while the compromised infrastructure is contained and signer set is rotated
Residual Risk	If the attacker gains access to 3 signing keys through the compromised infrastructure before detection, the scenario escalates to full multisig compromise (see Scenario 6)

SCENARIO 6: THREE OR MORE MULTISIG SIGNERS SIMULTANEOUSLY COMPROMISED

FIELD	DETAIL
Detection Method	Unauthorized transactions submitted and confirmed in the multisig; on-chain anomalies (unexpected large mints, implementation upgrades, mass blocklist changes); without real-time monitoring, detection may occur only after execution
Recovery Possible?	No
Recovery Authority	None: an attacker controlling 3 of 6 signing keys has full unilateral control of all privileged functions
Recovery Path	No on-chain recovery path; an attacker can mint arbitrary tokens, freeze or destroy holder funds, transfer ownership to an attacker-controlled address, or replace the implementation with malicious bytecode, all immediately with no timelock
Prerequisites / Dependencies	External intervention (legal, exchange delisting, community coordination) to limit impact; redeployment of a new contract
Operational Impact	Potentially catastrophic: all privileged functions are under attacker control
Residual Risk	High; the absence of a timelock means there is no on-chain reaction window for holders or the market; the 3-of-6 threshold is the primary defense and its effectiveness depends on signer independence and individual key management quality, neither of which is publicly documented

The multisig structure is appropriate for a token of this size and operational model. The 3-of-6 threshold provides resilience against single-signer failure and makes unilateral privileged action harder. However, the absence of a timelock removes any on-chain recovery window for holders. The greatest operational risks are permanent quorum loss (Scenario 2) and simultaneous compromise of 3 signers (Scenario 6), both of which are unrecoverable on-chain. The organization has not publicly documented recovery procedures, key backup arrangements, or emergency contact channels, which makes it impossible to assess off-chain failsafes from available evidence.

4.5 Multisig Security Analysis

The Gnosis MultiSigWallet at `0xc6cde7c39eb2f0f0095f41570af89efc2c1ea828` holds both implementation-owner and (via the ProxyAdmin) proxy upgrade authority. This section analyses it as an in-scope contract.

Contract: Gnosis MultiSigWallet (pre-Safe architecture, not the modern Gnosis Safe). Source code is verified on-chain.

Threshold: 3-of-6

Signer count: 6 (all EOAs)

Multisig entry points relevant to administrative authority:

FUNCTION	DESCRIPTION
`submitTransaction(address, uint256, bytes)`	Any owner can propose a transaction; does not execute immediately
`confirmTransaction(uint256)`	Owners confirm proposed transactions; auto-executes when threshold is reached if isConfirmed
`executeTransaction(uint256)`	Executes a confirmed transaction that was not auto-executed at confirmation
`revokeConfirmation(uint256)`	Allows an owner to withdraw a prior confirmation before execution
`addOwner(address)`	Adds a new signer; requires an on-chain multisig transaction
`removeOwner(address)`	Removes a signer; requires an on-chain multisig transaction
`replaceOwner(address, address)`	Replaces one signer with another; requires an on-chain multisig transaction
`changeRequirement(uint256)`	Modifies the confirmation threshold; requires an on-chain multisig transaction

Security posture: The pre-Safe Gnosis MultiSigWallet is a well-understood, audited implementation. It does not support modules, guards, or fallback handlers (features of the modern Safe architecture). All signer-set and threshold changes require an on-chain multisig transaction, providing auditability. All six signers are raw EOA keys; the security of each position depends entirely on off-chain key management (HSM, MPC, air gap, etc.) that is not publicly disclosed.

Signer independence: Geographic diversity, organizational independence, and infrastructure separation among the six signers are not publicly disclosed. If signers share infrastructure or are collocated, the effective security of the 3-of-6 threshold may be lower than its on-chain configuration implies. This cannot be assessed from available evidence.

Signing process security: No public disclosure of key management procedures, signing workflows, hardware security device usage, or approval processes for submitting transactions was found for TG Commodities or XAUT specifically.

Assessment: The pre-Safe Gnosis MultiSigWallet is a proven contract with no material security concerns at the bytecode level. The operational security of the multisig depends on the off-chain key management practices of the six individual EOA signers, which are undisclosed. The 3-of-6 threshold provides meaningful resistance to single-key compromise and requires coordinated multi-party action for all privileged operations, but the absence of timelock means confirmed transactions execute immediately with no advance notice.

5. Part III: Financial Analysis

Financial Risk Rating: Medium | Confidence: Medium

5.1 Underlying Asset Attestation

Attestation programme: BDO Advisory Services S.r.l. (Milan, Italy), quarterly, under ISAE 3000 (Revised) at the reasonable assurance level

Most recent attestation report: Q1 2026 Tether Gold Reserves Report (as of 31 March 2026), signed by Lelio Bigogno (Partner, BDO Advisory Services S.r.l.) on 30 April 2026, commissioned by Tether Global Investments Fund SICAF SA.

METRIC	VALUE	SOURCE
Gold held by custodian (Brinks and Loomis, Switzerland)	707,747.139 fine troy ounces	BDO attestation, 31 March 2026
XAUt tokens in circulation (all chains)	707,747.090 XAUt	BDO attestation, 31 March 2026
Treasury tokens (Alpha Group Commodities)	148,148.450 XAUt	BDO attestation, 31 March 2026
Tokens sold to market	559,598.640 XAUt	BDO attestation, 31 March 2026
Collateralisation ratio	100.000007% (surplus: 0.049 oz)	Derived from BDO figures
On-chain token supply (Ethereum, snapshot block 25042795)	707,747.089 XAUt	On-chain
Implied collateralisation ratio at snapshot	~100.000007%	Derived
Market price	USD 4,691.35 per XAUt	CoinGecko, DeFiLlama (cross-checked)
Circulating supply (CoinGecko, excluding treasury)	592,398.737 XAUt	CoinGecko
30-day average daily volume (CEX, conservative, excluding unverified outlier)	approx. USD 70–80 million	CoinGecko aggregated CEX data
30-day average daily volume (DEX, conservative executable)	approx. USD 57 million pool depth	DeFiLlama, Uniswap, on-chain

The Q1 2026 attestation confirms 707,747.139 fine troy ounces of physical gold against 707,747.090 XAUt tokens outstanding across all blockchains as of 31 March 2026. The Ethereum Mainnet on-chain supply at the assessment snapshot (707,747.089 XAUt) differs from the all-chain attestation figure by 0.001 XAUt, which is within the rounding precision of the attestation (six decimal places). This confirms that the entire issued supply resides on Ethereum Mainnet; any cross-chain issuance (for example, on BNB Chain) is negligible or zero.

The difference between the total on-chain supply (707,747.089 XAUt) and the CoinGecko circulating supply (592,398.737 XAUt), a gap of approximately 115,348 XAUt, is consistent with the treasury balance held by Alpha Group Commodities, S.A. de C.V. (148,148.450 XAUt as of 31 March 2026), reduced by approximately 32,800 XAUt of treasury sales in the six weeks between the attestation date and the snapshot date.

Gold bar inventory breakdown (31 March 2026):

BAR TYPE	QUANTITY	FINE TROY OUNCES
12.5 kg (LBMA Good Delivery)	1,759	706,975.587
1.0 kg	15	482.220
0.5 kg	18	289.332
Total	**1,792**	**707,747.139**

BDO's attestation procedures included independent inventory confirmation via a specialised precious metals provider, on-site inventory procedures, valuation verification using the LBMA gold price, and reconciliation of blockchain ledger balances to the accounting system. The attestation is conducted under ISAE 3000 (Revised) at the reasonable assurance level, which is a recognised and demanding independent standard.

Reserve adequacy conclusion: Reserves are fully adequate. For every XAUt token outstanding (707,747.090), the custodian holds at least one fine troy ounce of physical gold (707,747.139 oz). The 0.049-ounce surplus is negligible (approximately USD 230 at current gold prices). No reserve gap exists as of either the attestation date or the snapshot date.

Attestation quality limitations: The attestation is a point-in-time report covering 31 March 2026, published approximately 30 days after the period end. Individual bar serial numbers, refinery details, and vault sub-locations within Switzerland are not publicly disclosed, preventing independent third-party verification of the physical inventory beyond BDO's engagement. BDO Advisory Services S.r.l. is the world's fifth-largest accounting network but is not a Big 4 firm, which is a minor limitation relative to the asset's approximately USD 3.32 billion scale. The attestation is explicitly described as prepared "for transparency purposes" and may not be suitable for other purposes.

5.2 Counterparty Risk Profile

PARTY	ROLE	JURISDICTION	RISK SUMMARY
TG Commodities, S.A. de C.V.	Issuer	El Salvador	Tether subsidiary; no direct XAUT enforcement history; reputational risk from parent group's prior Tether-entity settlements
Alpha Group Commodities, S.A. de C.V.	Treasury / Distribution	El Salvador	Related party holding approximately 21% of total supply; large-sale overhang risk; no independent oversight
Brinks (Swiss operations)	Physical gold custodian	Switzerland	Established international vault operator; no known financial distress or regulatory sanctions
Loomis (Swiss operations)	Physical gold custodian	Switzerland	Established international vault operator; no known financial distress or regulatory sanctions
BDO Advisory Services S.r.l.	Attestor	Italy (BDO International member)	Independent ISAE 3000R attestor; top-5 accounting network; not Big 4

TG Commodities, S.A. de C.V. is incorporated in El Salvador (relocated from the British Virgin Islands in January 2025 under the Digital Asset Issuance Law) and is the sole issuer and redeemer of XAUt tokens. Its Sole Administrator is Giancarlo Devasini, who also serves as CFO of the Tether Holdings group. TG Commodities operates under a CNAD licence in El Salvador and a FinCEN MSB registration in the United States. Reputational risk is material: the parent group's entities (Tether Operations Limited, iFinex) were subject to CFTC and New York Attorney General settlements in 2021 related to USDT reserve disclosures and are unrelated to XAUT. No enforcement action or investigation directly targeting TG Commodities or XAUT has been identified. The issuer asserts that gold is "owned by XAUt token holders, not by the Company," establishing a property-law ownership claim. However, this has not been tested in insolvency proceedings under El Salvador law or Swiss custody law. No independent trustee, ring-fenced SPV, or statutory segregation mechanism exists to protect this claim independently of the issuer in a stress scenario.

Alpha Group Commodities, S.A. de C.V. is a related-party entity (also relocated from BVI to El Salvador in January 2025) that holds the treasury and unsold XAUt supply: approximately 148,148 XAUt as of 31 March 2026, representing approximately 21% of total issued supply. Large-scale sales from this treasury could increase available supply and exert downward pressure on secondary market prices. No public information on Alpha Group's mandate, sales restrictions, or oversight by independent directors was identified. This creates a potential overhang risk for secondary market price discovery.

Brinks and Loomis are established, globally-recognised professional vault and logistics operators with extensive experience in precious metals custody. Both operate in Switzerland, where their activities are subject to Swiss legal and regulatory requirements for professional custody. No known financial distress, sanctions exposure, or material operational failures in their Swiss precious metals custody businesses were identified. Both custodians provide geographic and operational diversification within a single jurisdiction; a systemic Swiss regulatory or legal event affecting gold exports could simultaneously impact both. Whether

the gold is held in segregated allocated accounts (consistent with bar-level inventory) or commingled unallocated accounts is not fully specified in the attestation; however, the bar-level breakdown (1,792 individually weighted bars) strongly implies allocated, bar-specific holdings.

BDO Advisory Services S.r.l. is the Italian member of BDO International Limited, the world's fifth-largest global accounting network. BDO Advisory Services S.r.l. attests that its engagement was conducted in accordance with ISAE 3000 (Revised), with independence per the IESBA Code of Ethics and quality management per ISQM1. The engagement is commissioned by Tether Global Investments Fund SICAF SA, a Tether group entity; however, formal ISAE 3000R attestor independence requirements are declared met. BDO's role is limited to assurance on the specific reserve figures; it does not provide a broader audit opinion on TG Commodities' financial condition.

5.3 Liquidity Risks and Scenario Analysis

5.3.1 LIQUIDITY PROFILE

Issuer redemption: Direct redemption with TG Commodities requires completed KYC/AML onboarding and a minimum redemption of approximately 430 XAUt (corresponding to one 12.5 kg LBMA Good Delivery bar, approximately USD 2.0 million at current prices). Physical bar delivery is Switzerland-only. The redemption fee is 0.25%. Settlement requires physical logistics and typically takes days to weeks from request to bar delivery. No published cash-settlement mechanism exists for retail redemptions. For holders below the minimum bar size or outside Switzerland, the secondary market is the only practical near-term exit.

DEX liquidity: Reported total DEX TVL across 43 pools is approximately USD 315.6 million. However, the majority is not freely executable for XAUT exits: approximately USD 125 million is in an institutional/restricted venue (multipli.fi), approximately USD 94.9 million is in lending pools (Aave v3, Morpho Blue, Aave v4, Fluid, Compound, Lista) where XAUT is posted as collateral and is not available for direct swap, and approximately USD 31.8 million is in protocols of uncertain executability. Conservative executable DEX liquidity from swap pools is approximately USD 57 million. The primary swap pools are:

VENUE	TYPE	TVL / DEPTH	NOTES
Uniswap v3, XAUT-USDT (0.05%)	DEX swap	~USD 15.9M	24h volume ~USD 5.9M; most liquid single exit pool
Uniswap v3, PAXG-XAUT (0.01%)	DEX swap	~USD 9.3M	24h volume ~USD 3.7M; cross-gold-token liquidity
Uniswap v4, PAXG-XAUT (0.05%)	DEX swap	~USD 6.6M	Additional cross-gold-token depth
Fluid DEX, PAXG-XAUT	DEX swap	~USD 4.0M	24h volume ~USD 0.14M
Uniswap v4, XAUT-USDC (0.30%)	DEX swap	~USD 3.9M	24h volume ~USD 0.23M
Curve and other swap pools	DEX swap	~USD 17M combined	Varied fee tiers and protocols

DEX pools are heavily weighted toward XAUT pairs against stablecoins and other gold-linked tokens, so secondary-market exit capacity depends on a small number of pools and routing paths rather than broad, deep spot-market liquidity. At USD 57 million conservative DEX depth versus approximately USD 3.32 billion total reserve value, DEX liquidity represents approximately 1.7% of reserves. This does not create a reserve adequacy concern and is not independently sufficient to drive the financial rating. The relevant liquidity risk is that smaller holders and non-Swiss holders rely primarily on secondary markets because direct issuer redemption is physical-only, minimum-size gated, and operationally slow. Normal and moderate-stress exits are supportable through DEX plus credible CEX liquidity, while coordinated large-scale exits require issuer redemption, OTC execution, or CEX order-book depth beyond the conservative DEX estimate.

CEX liquidity: Reported 24-hour CEX volume is approximately USD 156.9 million across 30 venues. CoinUp.io accounts for approximately USD 68.3 million of this total and has no trust score; its volume should not be relied upon. Excluding CoinUp.io, identifiable mid-to-large-venue CEX volume is approximately USD 70–80 million per day. Key venues include Binance (~USD 10.2M/day), OKX (~USD 13.4M/day), Gate (~USD 11.6M/day), and Bybit (~USD 9.2M/day). Kraken (~USD 1.3M/day) is the most relevant regulated US-accessible benchmark.

Combined short-term liquid exit capacity is in the range of USD 130–140 million per trading day (conservative DEX depth plus mid-to-large-venue CEX daily volume). This is adequate for normal and moderate-stress conditions but insufficient for a coordinated large-scale exit.

5.3.2 SCENARIO ANALYSIS

Scenario 1: Base Case

FIELD	DETAIL
Trigger Conditions	Normal operating environment; redemption demand within historical norms; collateral fully attested at 100%+ collateralisation
Effect on Collateral	Full 1:1 gold backing maintained; 0.049-oz surplus provides negligible but positive buffer; no collateral stress
Liquidity Runway	DEX depth (~USD 57M) and conservative CEX volume (~USD 70–80M/day) comfortably absorb ordinary redemption flow; direct issuer redemption processes physical requests at 0.25% fee with standard multi-day logistics
Anticipated Investor Actions	Normal holding and trading behavior; institutional subscribers and redeemers transact directly with the issuer; retail holders use secondary market
Conclusion	No liquidity constraint under normal conditions; reserve fully backed; token performs as designed
Impact	Low

Scenario 2: Market Stress (Gold Price Declines 20%)

FIELD	DETAIL
Trigger Conditions	A 20% gold price decline (e.g., from USD 4,691 to USD 3,753) driven by macroeconomic or commodity market stress; elevated redemption demand above historical norms
Effect on Collateral	Reserve USD value declines to approximately USD 2.66 billion; the 1:1 gold-ounce ratio is maintained because XAUT is denominated in gold ounces, not USD; no collateral shortfall arises from a price decline
Liquidity Runway	Elevated redemption demand (~5% of sold tokens, approximately USD 105M at reduced price) can be partially absorbed by DEX (~USD 57M); the remainder enters the issuer queue with multi-day settlement
Anticipated Investor Actions	USD-denomination holders experience mark-to-market losses; some holders may redeem or sell on secondary market; the gold-ounce parity ensures holders who redeem receive full physical backing
Conclusion	No structural insolvency; holder USD losses reflect commodity price movement; secondary market may see temporary spread widening as sell pressure increases relative to available DEX depth
Impact	Medium

Scenario 3: Bank Run (25% of Circulating Supply Redeemed Within 6 Hours)

FIELD	DETAIL
Trigger Conditions	A confidence shock (e.g., adverse news about TG Commodities or Tether group) triggers coordinated, rapid redemption of approximately 25% of circulating supply (~176,937 XAUt, approximately USD 830M at spot prices)
Effect on Collateral	Reserves remain fully backed in gold ounces; the constraint is operational throughput, not solvency
Liquidity Runway	Available DEX depth (~USD 57M) is overwhelmed; physical redemptions cannot process in 6 hours given minimum bar size, logistics, and settlement timelines; the issuer would need to gate the redemption queue
Anticipated Investor Actions	Holders unable to redeem directly sell on secondary market; XAUT likely trades at a 3–8% discount to spot gold during peak panic; arbitrage by direct-redemption-eligible counterparties partially bounds the discount
Conclusion	Reserves are fully solvent; the risk is operational and market-confidence driven; the absence of a cash-settlement option and the minimum bar-size requirement create meaningful secondary-market pressure during a coordinated exit
Impact	High

Scenario 4: Oracle Failure or Price Feed Manipulation

FIELD	DETAIL
Trigger Conditions	A primary gold price oracle (e.g., Chainlink XAU/USD) becomes stale or is manipulated for 15 or more minutes
Effect on Collateral	Physical reserve integrity is unaffected; oracle failure does not change the gold holdings backing the tokens
Liquidity Runway	Lending protocols using XAUT as collateral (Aave v3, Morpho Blue, Aave v4, Compound, Lista, approximately USD 91.4M combined) may freeze liquidations or accumulate bad debt if gold price moves materially during an oracle stale period; DEX swaps using oracle-priced liquidity may also be affected
Anticipated Investor Actions	Protocol-level: liquidations may be blocked or mis-priced; holder-level: redemption via issuer is unaffected (physically settled, not oracle-dependent)
Conclusion	Physical reserve integrity is not affected by oracle failure; DeFi integrations that rely on a XAU/USD price feed face secondary exposure, particularly for approximately USD 91.4M of XAUT posted as collateral in lending protocols
Impact	Medium

Scenario 5: Custodian Failure (48-Hour Processing Freeze)

FIELD	DETAIL
Trigger Conditions	A 48-hour custodial processing freeze at Brinks and/or Loomis due to operational disruption, regulatory action, or financial distress blocks all physical redemptions
Effect on Collateral	Gold is legally asserted to be owned by token holders, not TG Commodities; in a custodian insolvency scenario, token holders would need to assert ownership claims under Swiss custody law; the practical outcome of such claims is untested
Liquidity Runway	Secondary market becomes the sole near-term exit during the freeze; USD 57M DEX depth and conservative CEX volume (~USD 70–80M/day) provide partial relief for a USD 3.32B asset base
Anticipated Investor Actions	Holders unable to process physical redemptions sell on secondary market; XAUT likely trades at a 2–5% discount during the freeze as market-making uncertainty increases
Conclusion	The token-holder ownership claim is the primary protection against custodian insolvency; reserves should not form part of the custodian's insolvency estate if that claim is valid under applicable law, but it has not been tested; a prolonged custodian disruption could severely damage market confidence even if the underlying gold remains safe
Impact	High

5.4 Regulatory and Legal Jurisdiction

Issuer jurisdiction: El Salvador (Sociedad Anónima de Capital Variable)

Governing law: El Salvador law (pursuant to CNAD oversight); IFRS measurement principles applied to reserves reporting (recognition and measurement only)

REGULATORY ITEM	DETAIL
Primary regulator	Comisión Nacional de Activos Digitales (CNAD), El Salvador, under the Digital Asset Issuance Law (LEAD, enacted 2023)
Licence / registration	Stablecoin Issuer and Digital Asset Service Provider (DASP) licence under CNAD/LEAD; FinCEN MSB registration (US AML compliance only; not product approval)
AML / KYC framework	Bank Secrecy Act (BSA)/FinCEN for US obligations; El Salvador FIU (Unidad de Investigación Financiera) under LEAD; on-chain blacklisting for protocol-level enforcement
Enforcement history	None identified directly against TG Commodities or XAUT. Group-level: CFTC (2021) and New York AG (2021) settlements against Tether Operations Limited (USDT entity), not TG Commodities or XAUT.
Pending proceedings	None identified as of the assessment date

TG Commodities relocated from the British Virgin Islands to El Salvador in January 2025 to take advantage of El Salvador's Digital Asset Issuance Law (LEAD). The CNAD/LEAD framework is nascent (enacted 2023, operational since 2024) and, while it provides a formal legal basis for XAUT issuance, it lacks the institutional depth, enforcement history, cross-border recognition, and investor-protection frameworks of major G10 equivalents (FCA, FINMA, MAS, SEC). El Salvador was removed from the FATF grey list in February 2025, which reduces AML supervisory concerns relative to the 2022–2025 period. No equivalent to a ring-fenced statutory trust or bankruptcy-remote SPV exists under the CNAD framework; token-holder ownership claims rest on contractual and property-law assertions under El Salvador law that have not been judicially tested.

The most near-term material regulatory risk is MiCA non-compliance. XAUt is not registered under EU Regulation 2023/1114 (MiCA) and no approved white paper has been filed with any EU national competent authority. As a commodity-backed crypto-asset offered to the public, it may be subject to MiCA's Title II requirements. Issuers and distributors marketing or distributing XAUt in the EU without a compliant white paper may face regulatory scrutiny. MiCA's full application deadlines passed in late 2024 to 2025; enforcement timelines vary by member state. EU market access risk is the most concrete near-term regulatory exposure.

In the United States, the CFTC has asserted jurisdiction over commodity-backed tokens, and XAUt's gold backing places it clearly within the commodity domain. No CFTC registration or commodity pool exemption has been identified. Latent enforcement risk exists for US-person exposure, though no action has been initiated. The SEC has separately indicated interest in tokens resembling securities; XAUT's commodity structure is relatively distinct from the securities characterisation.

No licences or registrations have been identified in the United Kingdom (FCA), Singapore (MAS), Hong Kong (SFC), Japan (FSA), UAE (VARA), Australia (ASIC), or Switzerland (FINMA for the token itself; FINMA oversight of the Swiss vault custodians provides indirect comfort on the physical gold side). The absence of G10 regulatory coverage limits the addressable investor base and could restrict institutional distribution as global digital asset regulation matures.

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

XAUT presents a Moderate composite risk profile, driven by Medium conditions in both the operational and financial domains, with the smart contract domain assessed as Low risk. On the smart contract side, the proxy-implementation architecture is well-understood, both contracts have verified source and bytecode, formal verification confirmed no hidden calldata trapdoors, all 40 fork-based behavioral tests passed, and only two Low-severity administrative findings (SEC-01, SEC-02) were identified; this supports High smart-contract confidence. The operational risk is shaped by the absence of any on-chain timelock (all privileged actions execute immediately after 3-of-6 multisig confirmation with no holder notice window) and the non-disclosure of individual signer key management arrangements for all six EOA signers; this transparency gap is assessed as a Medium condition given the absence of any historical incident. The financial domain carries Medium risk despite strong reserve adequacy because holder exits depend on a constrained redemption structure and limited secondary-market depth under stress: direct redemption is minimum-size gated, physically settled, Switzerland-only, and lacks a published retail cash-settlement path; coordinated large exits would rely on issuer processing, OTC desks, or CEX liquidity rather than DEX liquidity alone. The rating is also supported by untested token-holder ownership claims under insolvency, the absence of an independent trustee or ring-fenced legal structure, a related-party treasury balance representing approximately 21% of issued supply at the latest attestation, and indirect reputational and counterparty exposure to the Tether Holdings group. Composite confidence is Medium: smart-contract evidence is strong and independently verifiable, but material off-chain evidence (signer key management, physical vault sub-account structure, bar-level inventory for independent cross-check) was unavailable, and the nascent CNAD regulatory framework reduces confidence in the legal enforceability of token-holder property rights under stress.

6.2 Improvement Suggestions

- **Operational security transparency:** TG Commodities does not publicly disclose its key management policy for the multisig signers, its recovery and incident response playbook (covering key loss, key compromise, quorum loss, and emergency pause scenarios), or its monitoring policy (events and

thresholds that trigger administrative alerts for the multisig and token contracts). Publicly disclosing these three elements, ideally in a dedicated security policy document, would materially improve the assessability of operational risk and increase confidence in the operational rating. For a USD 3.32B gold-backed token controlled by a 3-of-6 multisig, the absence of any public operational security disclosure is a significant transparency gap.

- **Reserve transparency:** Publishing the individual gold bar list (LBMA bar serial numbers, weights, and refinery codes) in a machine-readable format alongside each quarterly reserves report would enable independent third-party verification of the attested inventory and increase financial confidence. This practice is consistent with disclosure standards expected of large commodity-backed token issuers by institutional investors.
- **Token-holder ownership claim formalisation:** The assertion that gold is "owned by token holders, not by the Company" rests on contractual and property-law claims that have not been tested in judicial proceedings. Establishing a formal trust deed, statutory ring-fence, or equivalent legal structure, verified by independent legal opinion under El Salvador law and Swiss custody law, would materially strengthen the position of token holders in a stress or insolvency scenario.
- **MiCA compliance pathway:** TG Commodities has not obtained MiCA authorisation or published an approved crypto-asset white paper under EU Regulation 2023/1114. Engaging with an EU national competent authority to establish a compliance pathway, even if XAUT is ultimately classified under a Title II exemption, would reduce regulatory risk for EU-based distributors and holders and expand the addressable institutional investor base.

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 of the proxy or implementation contract
- A change to any privileged role holder identified in section 4.1, including changes to multisig signers or threshold
- A material change to the custodian, redemption model, reserve composition, issuer legal structure, or primary regulatory jurisdiction identified in sections 5.1 through 5.4
- 12 months from the date of publication
