Meridion Risk Assessment: PAX Gold (PAXG)

FIELD	VALUE
Digital Asset	PAX Gold (PAXG)
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

PAX Gold (PAXG) is a commodity-backed digital asset issued by Paxos Trust Company, LLC, in which each token represents exactly one fine troy ounce of an LBMA Good Delivery gold bar held in segregated, allocated custody at LBMA-accredited vaults in London. PAXG was approved by the New York Department of Financial Services on 5 September 2019. Paxos received conditional OCC approval on 12 December 2025 to convert to a national trust bank, subject to satisfying OCC conditions; final completed conversion was not independently confirmed in this assessment. Its principal use cases are gold price exposure, portfolio diversification, and DeFi collateral. PAXG is issued exclusively on Ethereum Mainnet by Paxos; non-Ethereum representations observed on Solana and Polkadot are third-party wrapped tokens not issued or backed by Paxos. At the assessment snapshot block 25042795 (2026-05-07), the on-chain total supply was 479,162.743 PAXG, representing a reserve value of approximately $2.262 billion at the prevailing spot price of $4,721.02 per troy ounce.

KYC Gating

Secondary-market holding of PAXG does not require KYC with Paxos; any Ethereum address may receive and hold PAXG without registering with the issuer. Minting is KYC-gated: direct creation of PAXG through Paxos requires passing Paxos KYC and AML onboarding and being an approved customer. Redemption for physical gold (minimum 430 PAXG per Good Delivery bar) or USD cash requires the same Paxos KYC approval. An on-chain freeze and balance-wipe mechanism exists in the contract, controlled by the `assetProtectionRole` (currently the EOA `0x3af3e85f4f97de7ad0f000b724fb77fe5ffc024b`); this role can block all transfers to and from any address and permanently destroy the token balance held at a frozen address, reducing total supply. Paxos exercises this capability in response to OFAC sanctions lists and legal orders. Secondary-market transfers on DEX platforms and CEX exchanges are not gated by Paxos KYC directly, though CEX platforms impose their own KYC at the exchange level.

Overall Risk Rating: Low

Composite Confidence: Low

The composite Low rating reflects a single domain at Medium (operational security) under conditions that are contingent and not currently causing holder harm. The proxy admin, owner and asset-protection role, and supply controller are all confirmed bare externally owned accounts operating over approximately $2.262 billion in token value with no on-chain timelocks, no second-approval requirements, and no publicly disclosed key management controls such as HSM custody or MPC arrangements; however, no operational incident involving key compromise, unauthorised minting, or misuse of administrative authority has been recorded in six years of operation. The smart contract domain is rated Low: the deployed code is well-structured, FV-confirmed for hidden calldata surface, and presents only a single Low-severity finding (SEC-01). The financial domain is rated Low: PAXG's 1:1 gold-oz backing is structurally sound, and monthly KPMG LLP examination reports provide independent reserve support. Paxos's conditional OCC approval is a positive regulatory development, but it is not treated as a completed charter in this rating. Composite confidence is Low, driven by the absence of publicly disclosed key management evidence for the three confirmed highest-privilege EOA roles.

Smart Contract Security Summary

SEVERITY	COUNT	RESOLVABLE
Critical	0	0
High	0	0
Medium	0	0
Low	1	1

The smart contract review identified one Low-severity finding (SEC-01): an event-log bug in `setBetaDelegateWhitelister` where storage is written before the event is emitted, causing the `oldWhitelister` argument in the `BetaDelegateWhitelisterSet` event to reflect the new value rather than the previous holder. No on-chain funds are at risk; the finding affects only monitoring and audit-trail infrastructure. The upgrade proxy mechanics, access-control modifiers, signature replay protection for delegated transfers, supply accounting, and asset-protection functions are all correctly implemented. Formal verification of the deployed bytecode confirmed the complete absence of hidden selector-based trapdoors and malformed-calldata attack surfaces for both the proxy and the implementation. Fork-based behavioral tests covering all 57 required cases across both contracts passed at the assessment snapshot block, confirming that deployed bytecode behaves consistently with the reviewed source for representative positive and negative call paths.

Smart Contract Risk Score: Low | Confidence: High

Operational Security Summary

PAXG's operational security is rated Medium. The proxy admin (`0xc94bcf6e1d8b3558e3b62e743630d50497e3851c`) holds unilateral authority to replace the entire implementation contract in a single transaction with no timelock; it is a confirmed bare externally owned account with no deployed bytecode and no disclosed key management arrangement. The owner and asset-protection role are consolidated in a single EOA (`0x3af3e85f4f97de7ad0f000b724fb77fe5ffc024b`), which alone controls pause, freeze, and irreversible balance destruction over the full token supply. The supply controller (`0x2fb074fa59c9294c71246825c1c9a0c7782d41a4`) is also an EOA with unbounded, single-transaction minting authority and no on-chain approval gate. None of these roles carry a publicly disclosed key management policy. The fee controller function is the exception: it is held by a smart contract (`0x0644bd0248d5f89e4f6e845a91d15c23591e5d33`), reducing EOA concentration for fee operations. Confidence is Low because none of the highest-privilege EOAs have disclosed HSM or MPC custody, threshold controls, emergency workflow, or change-control procedures.

Opsec Risk Score: Medium | Confidence: Low

Financial Summary

PAXG's financial risk is rated Low. Each token is backed 1:1 by physical gold held in allocated, segregated LBMA vaults, eliminating fractional-reserve and maturity-mismatch risk inherent in fiat-backed stablecoins. Gold reserves are attested monthly by KPMG LLP under AICPA examination-level standards; the April 2026 report was confirmed available on the Paxos transparency page at assessment time. Paxos received

conditional OCC approval on 12 December 2025 to convert to a national trust bank; the conditionally approved conversion is treated as positive but not as completed federal charter status for this assessment. The primary financial risk factors are: secondary market liquidity that is modest relative to total supply (conservative executable DEX depth of $55.7M versus $2.262B reserve value, ranking strongest among the three reviewed reports at approximately 2.46% of reserve value); the undisclosed allocation split between the two London custodians, Brink's Global Services Ltd. and ICBC Standard Bank Plc, preventing precise concentration assessment; and legal uncertainty over whether token holders can directly enforce property rights in specific bars rather than relying on contractual redemption rights against Paxos in an insolvency scenario. Confidence is Medium because the custodian allocation split between the two London vaults is undisclosed, preventing precise concentration assessment.

Financial Risk Score: Low | Confidence: Medium

Scope Limitations

- **Non-Ethereum third-party wrapped representations:** PAXG-derived tokens on Solana (Raydium IMT-PAXG) and Polkadot (Hydration) are third-party wrapped tokens and were excluded from scope. These do not create additional Paxos gold obligations and have no rating effect on the present assessment; they may carry independent smart-contract or bridge risk not assessed here. Confidence effect: none for this report.
- **FeeController contract internals (`0x0644bd0248d5f89e4f6e845a91d15c23591e5d33`):** The internal governance of the fee controller contract (signer structure, quorum, upgrade authority) was not assessed in this engagement. Given the limited severity of fee-rate manipulation, this is not expected to change the opsec domain rating. Confidence effect: reduces confidence in the fee-control sub-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: 25042795 (2026-05-07)

CONTRACT	ROLE	ADDRESS	COMPILER
AdminUpgradeabilityProxy	Proxy	`0x45804880De22913dAFE09f4980848ECE6EcbAf78`	`0.4.24+commit.e67f0`
PAXGImplementation	Implementation	`0x74271F2282eD7eE35c166122A60c9830354be42a`	`v0.4.24+commit.e67f`

Both contracts are verified on Blockscout. The proxy is an `AdminUpgradeabilityProxy` from the ZeppelinOS pre-EIP-1967 era, using keccak256-derived unstructured storage slots for the admin and implementation pointers. The implementation is `PAXGImplementation`, the single logic contract underpinning all PAXG token operations. Both contracts were compiled with Solidity 0.4.24, optimization enabled (200 runs), and the proxy with the `byzantium` EVM version. All addresses were verified against on-chain deployment artifacts.

3.2 Entry Point Catalogue

The entry-point catalogue was reconstructed from deployed bytecode and verified source artifacts. All 54 runtime-reachable ABI entries were covered (comparison script status: PASS, zero missing, zero duplicates). The catalogue serves as the exclusion set for hidden-surface formal verification.

Proxy contract entry points:

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
EP-PR-001	`changeAdmin(address)`	`ifAdmin` (proxy admin only)	High	Transfers proxy administration to a new address. Changing the admin transfers the exclusive right to upgrade the implementation and change the admin itself. Zero-address input reverts. Compromise of this key is equivalent to full protocol control over all PAXG balances.
EP-PR-002	`upgradeTo(address)`	`ifAdmin` (proxy admin only)	High	Upgrades the proxy to a new implementation address. Overwrites the ZeppelinOS implementation storage slot. Target address must be a deployed contract (extcodesize check). A compromised admin can replace the entire token logic with arbitrary bytecode, enabling fund theft or supply manipulation.
EP-PR-003	`upgradeToAndCall(address,bytes)`	`ifAdmin` (proxy admin only)	High	Upgrades the proxy to a new implementation and immediately calls a function on it via `address(this).call(data)`. The inner call re-enters the proxy fallback with `msg.sender == proxy address`. Future upgrade initialisers that set `owner = msg.sender` would set the owner to the proxy address, permanently bricking administrative functions; explicit owner arguments must be passed instead.
EP-PR-004	`fallback()`	Public (non-admin callers only; `_willFallback` reverts if admin)	Medium	Routes all calls that do not match proxy-admin selectors, or where `msg.sender` is not the admin, to the current implementation via delegatecall. Primary execution path for all token operations. Accepts ETH (payable).

The proxy contract includes 2 additional functions that are not state-modifying (view): `admin()` (EP-PR-005) and `implementation()` (EP-PR-006).

Implementation contract entry points:

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTI
EP-IM-001	`betaDelegatedTransfer(...) [6 args]`	`onlyBetaDelegate` (whitelisted caller)	High	Executes a transfer on b holder identi EIP-712 sig signature le malleability v must be 2 deadline (bl per-address number (rep and freeze a Transfers va and servicel
EP-IM-002	`betaDelegatedTransferBatch(...) [8 args]`	`onlyBetaDelegate` (whitelisted caller)	High	Executes an delegated tr validated as All array len match; a sin transfer reve batch. Large approach bl but batch siz by the white
EP-IM-003	`decreaseSupply(uint256)`	`onlySupplyController`	High	Burns token supply contr reducing bot and `totals` Operates re pause state SafeMath pr underflow. A supply-contr unrestricted destruction.
EP-IM-004	`freeze(address)`	`onlyAssetProtectionRole`	High	Freezes the address, blo transfers to Operates re pause state. address is a Currently ga EOA which a asset-protec
EP-IM-005	`increaseSupply(uint256)`	`onlySupplyController`	High	Mints new to supply contr and increase

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTI
				`totalSupp` in the contra regardless c compromise controller ke unlimited tok
EP-IM-006	`pause()`	`onlyOwner`	High	Pauses all tr `transferF` `approve` , `betaDeleg` operations. S and asset pr unaffected. already paus
EP-IM-007	`transfer(address,uint256)`	Public (`whenNotPaused` , freeze checks)	High	Standard ER Enforces pa recipient, fre both sender and balance fee (feeRate transfer amo and credited Currently fee
EP-IM-008	`transferFrom(address,address,uint256)`	Public (`whenNotPaused` , requires prior approval)	High	Standard ER transferFrom approval fro address. En non-zero rec checks on and `msg.s` and allowan Allowance is before the tr effects order
EP-IM-009	`unpause()`	`onlyOwner`	High	Resumes al operations. already unpa
EP-IM-010	`wipeFrozenAddress(address)`	`onlyAssetProtectionRole`	High	Permanently tokens held address, rec address bala `totalSupp` must already Operates re pause state.

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTI
				by the wipe but are harm balance is z
EP-IM-011	`approve(address,uint256)`	Public (`whenNotPaused` , freeze checks)	Medium	Sets the allo spender. Th ERC-20 app condition ap (documente comments); increaseAllo decreaseAll are provide
EP-IM-012	`claimOwnership()`	Proposed owner only	Medium	Completes t ownership tr by `propos` owner to pro and clears p Prevents ac to an inacce
EP-IM-013	`initialize()`	Public (initialized guard)	Medium	Initialises co owner, supp feeControlle feeRecipien `msg.sende` the EIP-712 separator; s `initializ` Reverts on a The implem constructor function ther `pause()` , implementat pre-initialise
EP-IM-014	`proposeOwner(address)`	`onlyOwner`	Medium	Initiates the ownership tr recording th owner. Reve proposed ow the current
EP-IM-015	`reclaimPAXG()`	`onlyOwner`	Medium	Transfers an the proxy co to the owner pause or fre Useful for re

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTI
				accidentally proxy addre
EP-IM-016	`setAssetProtectionRole(address)`	`onlyAssetProtectionRole` or owner	Medium	Sets the add to freeze, un frozen addre zero address the freeze ca
EP-IM-017	`setBetaDelegateWhitelister(address)`	`onlyOwner`	Medium	Sets the add to whitelist c beta delegat event-log bu storage is w event is emi `oldWhitel` argument to value.
EP-IM-018	`setSupplyController(address)`	`onlySupplyController` or owner	Medium	Sets the add to mint and Callable by t supply contr owner. Reve address. Em assignment correctly cap
EP-IM-019	`unfreeze(address)`	`onlyAssetProtectionRole`	Medium	Removes th address, res to send and Reverts if ad currently fro
EP-IM-020	`whitelistBetaDelegate(address)`	`onlyBetaDelegateWhitelister`	Medium	Adds an add delegate wh the ability to signed deleg Reverts if al whitelisted.
EP-IM-021	`disregardProposeOwner()`	Owner or proposedOwner	Low	Cancels a p ownership p resetting pro zero. Revert proposal exi
EP-IM-022	`initializeDomainSeparator()`	Public (no access gate)	Low	Recomputes EIP-712 dor the contract and the prox

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTI
				Output is de immutable p calling this f produces th and poses n
EP-IM-023	`setFeeController(address)`	`onlyFeeController` or owner	Low	Sets the add to set fee ra recipient. Th is currently a Reverts on z
EP-IM-024	`setFeeRate(uint256)`	`onlyFeeController`	Low	Sets the per in parts per 1,000,000 = Currently ga controller co 1,000,000 w full transfer feeRecipien
EP-IM-025	`setFeeRecipient(address)`	`onlyFeeController`	Low	Sets the add receives tra by the fee c contract. Re address.
EP-IM-026	`unwhitelistBetaDelegate(address)`	`onlyBetaDelegateWhitelister`	Low	Removes ar the beta-del revoking its delegated tr if address is

The implementation contract includes 22 additional functions that are not state-modifying (view or pure): EP-IM-027 through EP-IM-048.

Long function signatures in the table above are abbreviated as `name(...) [N args]`, where `N` is the total parameter count.

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 (KECC
AdminUpgradeabilityProxy	Proxy	`0x45804880De22913dAFE09f4980848ECE6EcbAf78`	`0xdcdc97bea54363548`
PAXGImplementation	Implementation	`0x74271F2282eD7eE35c166122A60c9830354be42a`	`0x493edc50f59a806ab`

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 of entrypoints (6 proxy entries, 48 implementation entries) serves as the exclusion set for hidden-surface verification. The report table in Section 3.2 covers state-modifying entry points only; all 54 runtime selectors were used in the FV exclusion set.

AdminUpgradeabilityProxy: Bytecode Surface Cases

Formal verification of the deployed AdminUpgradeabilityProxy 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

All feasible paths for unknown selectors and short calldata either delegate to the fixed implementation address `0x74271f2282ed7ee35c166122a60c9830354be42a` or revert. No unexpected non-reverting hidden behavior was found. Two execution paths were modelled in each case: one delegatecall path and one revert path.

PAXGImplementation: Bytecode Surface Cases

Formal verification of the deployed PAXGImplementation 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 paths for unknown selectors and short calldata in the implementation always revert. One execution path was modelled in each case. No unexpected non-reverting hidden behavior was found.

Overall verdict: CONFIRMED

3.3.2 FORK-BASED BEHAVIORAL TESTS

Fork-based behavioral tests were executed against the deployed AdminUpgradeabilityProxy `0x45804880De22913dAFE09f4980848ECE6EcbAf78` and PAXGImplementation `0x74271F2282eD7eE35c166122A60c9830354be42a` on an Ethereum mainnet Foundry fork at block 25042795.

ENTRY POINT	FUNCTION	POSITIVE TEST	NEGATIVE TEST
EP-PR-001	`changeAdmin`	PASS: proxy admin successfully transfers admin authority to a new address	PASS: non-admin call reverts
EP-PR-002	`upgradeTo`	PASS: proxy admin upgrades to a new implementation address	PASS: non-admin call reverts
EP-PR-003	`upgradeToAndCall`	PASS: proxy admin upgrades and executes initializer data atomically; full transaction reverts if inner call fails	PASS: non-admin call reverts
EP-IM-001	`betaDelegatedTransfer`	PASS: whitelisted delegate executes a pre-signed transfer on behalf of a token holder, including full EIP-712 signature construction, sequence-number enforcement, and deadline validation	PASS: non-whitelisted caller reverts
EP-IM-002	`betaDelegatedTransferBatch`	PASS: whitelisted delegate executes an atomic batch of pre-signed transfers; a single failed transfer reverts the entire batch	PASS: non-whitelisted caller reverts
EP-IM-003	`decreaseSupply`	PASS: supply controller burns tokens from own balance and totalSupply decreases accordingly	PASS: unauthorised caller reverts
EP-IM-004	`freeze`	PASS: assetProtectionRole freezes a target address, blocking all transfers	PASS: unauthorised caller reverts
EP-IM-005	`increaseSupply`	PASS: supply controller mints new tokens to own balance and totalSupply increases accordingly	PASS: unauthorised caller reverts
EP-IM-006	`pause`	PASS: owner successfully pauses all transfer, approve, and delegated-transfer operations	PASS: unauthorised caller reverts
EP-IM-007	`transfer`	PASS: succeeds for a non-frozen sender with sufficient balance; fee deducted at current feeRate	PASS: reverts when sender has insufficient balance
EP-IM-008	`transferFrom`	PASS: succeeds with valid prior allowance and sufficient balance; allowance decremented before transfer executes	PASS: reverts without prior allowance
EP-IM-009	`unpause`	PASS: owner successfully resumes all paused token operations	

ENTRY POINT	FUNCTION	POSITIVE TEST	NEGATIVE TEST
			PASS: unauthorised caller reverts
EP-IM-010	`wipeFrozenAddress`	PASS: assetProtectionRole permanently destroys balance of a frozen address and totalSupply decreases	PASS: reverts when target address is not currently frozen
EP-IM-011	`approve`	PASS: caller sets spender allowance when not paused and neither party is frozen	PASS: reverts when the spender is frozen
EP-IM-012	`claimOwnership`	PASS: proposed owner completes the two-step ownership transfer	PASS: non-proposed-owner call reverts
EP-IM-013	`initialize`	N/A: live deployment has already been initialised; positive execution path is permanently unavailable	PASS: repeat initialisation call reverts
EP-IM-014	`proposeOwner`	PASS: owner initiates two-step ownership transfer to a proposed address	PASS: unauthorised caller reverts
EP-IM-015	`reclaimPAXG`	PASS: owner recovers PAXG tokens held at the proxy contract address	PASS: unauthorised caller reverts
EP-IM-016	`setAssetProtectionRole`	PASS: owner reassigns the assetProtectionRole to a new address	PASS: unauthorised caller reverts
EP-IM-017	`setBetaDelegateWhitelister`	PASS: owner sets a new betaDelegateWhitelister address	PASS: unauthorised caller reverts
EP-IM-018	`setSupplyController`	PASS: owner reassigns the supplyController to a new address	PASS: unauthorised caller reverts
EP-IM-019	`unfreeze`	PASS: assetProtectionRole removes the freeze from an address, restoring transfer ability	PASS: reverts when target address is not currently frozen
EP-IM-020	`whitelistBetaDelegate`	PASS: betaDelegateWhitelister adds an address to the beta-delegate whitelist	PASS: unauthorised caller reverts
	`disregardProposeOwner`		

ENTRY POINT	FUNCTION	POSITIVE TEST	NEGATIVE TEST
EP-IM-021		PASS: owner cancels a pending ownership proposal, resetting proposedOwner to zero	PASS: reverts when no pending ownership proposal exists
EP-IM-022	`initializeDomainSeparator`	PASS: EIP-712 domain separator recomputed and stored from immutable proxy address and contract name hash	PASS: repeat call after domain separator is set reverts
EP-IM-023	`setFeeController`	PASS: feeController reassigns the feeController role to a new address	PASS: unauthorised caller reverts
EP-IM-024	`setFeeRate`	PASS: feeController sets the per-transfer fee rate in parts per million	PASS: unauthorised caller reverts
EP-IM-025	`setFeeRecipient`	PASS: feeController sets the address that receives transfer fees	PASS: unauthorised caller reverts
EP-IM-026	`unwhitelistBetaDelegate`	PASS: betaDelegateWhitelister removes an address from the beta-delegate whitelist	PASS: reverts when target address is not currently whitelisted

The proxy fallback (EP-PR-004) was not counted as a separate required case because it is not a named selector. It was exercised implicitly by every implementation entry-point test, since those calls were sent through the deployed proxy and therefore traversed the fallback delegatecall path.

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 (57/57 required cases passed; 28 positive cases, 29 negative cases, all 29 named entry points covered)

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 deployed bytecode performs representative intended operations and rejects representative invalid operations.

The formal verification results are fully confirmed for both contracts: the proxy routes unknown calldata exclusively to the fixed implementation or reverts, and the implementation rejects all unknown selectors and malformed calldata. This materially reduces the risk of hidden selector-based or malformed-calldata trapdoors in the deployed bytecode. Fork-based behavioral tests further confirmed that the deployed bytecode executes

all 57 representative intended and negative call paths correctly, providing sampled behavioural assurance across the complete entry-point surface. Together, formal verification and fork tests provide High confidence that the deployed bytecode matches the reviewed source with no material hidden behaviour.

3.4 Edge-Case Analysis

Edge-case analysis was conducted for all Critical and High entry points. Key findings are summarised below.

EDGE CASE	STATUS	EVIDENCE
changeAdmin: zero address input	Safe	`require(newAdmin != address(0))` in changeAdmin. Non-admin callers routed to implementation fallback.
upgradeTo: non-contract or EOA address	Safe	`AddressUtils.isContract` (extcodesize check) in `_setImplementation` reverts if target is not a deployed contract.
upgradeToAndCall: inner call failure reverts upgrade	Safe	`require(address(this).call.value(msg.value)(data))` failure causes full transaction revert including the implementation slot write.
upgradeToAndCall: msg.sender in inner call	Safe (operational note)	Inner call re-enters proxy with `msg.sender == proxy address`. Any future initialiser setting `owner = msg.sender` would set owner to the proxy address. Not a current exploit; must be accounted for in future upgrade procedures.
betaDelegatedTransfer: signature replay prevention	Safe	Per-address sequence numbers (nextSeqs) increment after each transfer. Deadline (block.number) prevents indefinite validity. Signature malleability mitigated via s-value bound and v in {27, 28}.
betaDelegatedTransfer: pause and freeze enforcement	Safe	`whenNotPaused` check in `_betaDelegatedTransfer`; frozen sender or recipient reverts.
betaDelegatedTransferBatch: array length mismatch	Safe	Two explicit length checks revert on mismatch before any transfers execute.
increaseSupply: no whenNotPaused guard	Safe	Intentional design; minting remains available during emergency pause so that reserve adjustments are not blocked. SafeMath prevents uint256 overflow on totalSupply.
decreaseSupply: underflow protection	Safe	`SafeMath.sub` reverts if burn amount exceeds the supply controller's balance. Operates regardless of pause state by design.
freeze: already-frozen address	Safe	`require(!frozen[_addr], "address already frozen")` reverts on duplicate freeze.
transfer: zero-address recipient	Safe	`require(_to != address(0))` reverts.
transfer: fee calculation overflow	Safe	`SafeMath.mul` and `SafeMath.div` wrap all fee arithmetic; practical balances are far below uint256 max.
transferFrom: allowance decremented before transfer	Safe	Allowance subtracted from `allowed[_from][msg.sender]` before `_transfer` executes, following checks-effects order.
transferFrom: frozen spender blocks spend	Safe	`require(!frozen[msg.sender])` reverts for a frozen spender even if a prior allowance exists.
wipeFrozenAddress: address not frozen	Safe	

EDGE CASE	STATUS	EVIDENCE
		`require(frozen[_addr], "address is not frozen")` reverts. Zero-balance wipe is a no-op (emits events with value 0).
pause: already paused	Safe	`require(!paused, "already paused")` reverts.
unpause: already unpaused	Safe	`require(paused, "already unpaused")` reverts.

3.5 Common Exploit Negatives

EXPLOIT CLASS	STATUS	EVIDENCE
Reentrancy	Mitigated	No external calls in any token operation. `_transfer` updates balances before emitting events and makes no callbacks. `betaDelegatedTransfer` uses `ecrecover` (a precompile, not an external call). No ERC-777 hooks.
Integer overflow / underflow	Mitigated	Solidity 0.4.24 with `SafeMath` applied throughout: `using SafeMath for uint256` declared in PAXGImplementation. All add, sub, mul, and div operations route through SafeMath and revert on overflow or underflow.
Access control bypass	Mitigated	Each privileged function is guarded by a modifier: `onlyOwner`, `onlySupplyController`, `onlyAssetProtectionRole`, `onlyFeeController`, `onlyBetaDelegateWhitelister`. The proxy's `ifAdmin` modifier routes non-admin callers to the implementation. No bypass path was identified.
Front-running	Mitigated	PAXG is a simple ERC-20 with no AMM or price-sensitive logic. The classic ERC-20 approve race condition applies (documented in contract comments) but is not unique to this implementation. `betaDelegatedTransfer` uses block.number deadlines and sequence numbers, which are not meaningfully front-runnable.
Oracle manipulation	Not applicable	PAXG has no on-chain price oracle dependency in any contract logic. Supply is controlled by Paxos off-chain via the `supplyController` role. No flash-loan-susceptible price-sensitive logic exists in the contract.
Signature replay	Mitigated	`betaDelegatedTransfer` uses EIP-712 typed data with per-address sequence numbers (nextSeqs) incremented after each use. Deadline enforcement (block.number) and the domain hash binding to the proxy address prevent cross-contract replay. Signature malleability is mitigated by s-value bound and v-value restriction. Note: the domain does not include chainId (pre-EIP-155 era).
Flash loan attack	Not applicable	No price-sensitive, collateral-ratio, or AMM logic in the contract. No flash-loan-exploitable mechanism was identified.
Denial of service	Mitigated	`betaDelegatedTransferBatch` contains an unbounded loop, but the caller must be a whitelisted delegate. All other functions are O(1). Block gas limit constrains batch size in practice.

3.6 Security Findings Register

SEC-01: SETBETADELEGATEWHITELISTER EMITS EVENT WITH INCORRECT OLD-VALUE ARGUMENT

FIELD	DETAIL
Finding ID	SEC-01
Title	setBetaDelegateWhitelister emits event with incorrect old-value argument
Severity	Low
Entry Point(s)	EP-IM-017 (`setBetaDelegateWhitelister`)
Description	In `PAXGImplementation.setBetaDelegateWhitelister()` , the storage variable `betaDelegateWhitelister` is assigned to `_newWhitelister` before the `BetaDelegateWhitelisterSet` event is emitted. The event signature is `BetaDelegateWhitelisterSet(address indexed oldWhitelister, address indexed newWhitelister)` . Because the storage write precedes the emit, both arguments resolve to `_newWhitelister` . The previous whitelister address is not captured in the event log.
Impact	No on-chain funds are at risk. Off-chain tooling that reads `BetaDelegateWhitelisterSet` logs to reconstruct whitelister history receives the same address for both old and new arguments, making it impossible to determine the previous holder from the event log alone. Severity is capped at Low because the function is access-controlled (`onlyOwner`) and the on-chain state transition is correct.
Recommendation	Capture the old value into a local variable before updating storage, then pass the local variable as the first argument to the event. Audit all similar role-setter functions (`setAssetProtectionRole` , `setSupplyController` , `setFeeController` , `setFeeRecipient` , `setFeeRate`) for the same pattern at the next upgrade opportunity.

4. Part II: Operational Security

Operational Security Rating: Medium | Confidence: Low

4.1 Privileged Roles

Role holders at assessment snapshot:

ROLE	ADDRESS	TYPE
Proxy Admin	`0xc94bcf6e1d8b3558e3b62e743630d50497e3851c`	EOA
Owner	`0x3af3e85f4f97de7ad0f000b724fb77fe5ffc024b`	EOA
AssetProtectionRole	`0x3af3e85f4f97de7ad0f000b724fb77fe5ffc024b`	EOA (same as owner)
SupplyController	`0x2fb074fa59c9294c71246825c1c9a0c7782d41a4`	EOA
FeeController	`0x0644bd0248d5f89e4f6e845a91d15c23591e5d33`	Contract
BetaDelegateWhitelister	Not observed in on-chain event history	Unknown
ProposedOwner	`0x0000000000000000000000000000000000000000`	Unset (zero address)

Proxy Admin (`0xc94bcf6e1d8b3558e3b62e743630d50497e3851c`): This is the highest-privilege role in the system. It holds exclusive authority to call `upgradeTo` and `upgradeToAndCall` on the proxy, enabling atomic replacement of the entire token implementation in a single transaction with no timelock and no second approval. A hostile or compromised proxy admin can replace the implementation with arbitrary bytecode; because the proxy executes via delegatecall, a malicious implementation has full read-write access to all proxy storage slots, including all PAXG balances. On-chain code verification confirms this address is a bare externally owned account with no deployed bytecode. With no on-chain governance contract mediating upgrade actions, the operational security of the proxy upgrade path depends entirely on off-chain key management controls for this single private key. No public disclosure of key management arrangements for this address is available. **Confidence effect: lowers operational confidence to Low.**

Owner and AssetProtectionRole (`0x3af3e85f4f97de7ad0f000b724fb77fe5ffc024b`): Confirmed EOA. The owner role controls: pause and unpause; initiating and completing two-step ownership transfer; setting or overriding the `assetProtectionRole`, `supplyController`, `feeController`, and `betaDelegateWhitelister`. The `assetProtectionRole` controls: freeze (blocks all transfers from and to any address); unfreeze; and `wipeFrozenAddress` (permanently destroys the full PAXG balance at a frozen address, reducing `totalSupply_`). Both roles are consolidated in a single EOA, meaning one key controls pause, freeze, and irreversible balance destruction over the full circulating supply. From May 2021 to August 2025, these roles were held by the fee controller smart contract, providing a layer of on-chain governance. The August 2025 reorganisation transferred them to this EOA, reducing on-chain control sophistication for these functions. Key management details (HSM, MPC, or equivalent) are not publicly disclosed. **Confidence effect: lowers operational confidence to Low.**

SupplyController (`0x2fb074fa59c9294c71246825c1c9a0c7782d41a4`): Confirmed EOA. Powers: `increaseSupply` (mint any quantity of PAXG in a single transaction; no ceiling in the contract); `decreaseSupply` (burn from the supply controller's own balance); `setSupplyController` (self-reassign the role independent of the owner). A compromised supply-controller key can mint the entire token supply, approximately $2.262 billion at assessment date, in a single transaction with no on-chain approval gate. The role has rotated three times since deployment, most recently in December 2024. Key management not publicly disclosed. **Confidence effect: lowers operational confidence to Low.**

FeeController (`0x0644bd0248d5f89e4f6e845a91d15c23591e5d33`): Confirmed contract. Powers: set fee rate (0 to 100% of transfer value); set fee recipient; reassign the fee controller role. Fee-rate manipulation cannot drain existing balances directly; it can only redirect future transfer fee flows. This is the only role currently held by a smart contract, which reduces single-EOA concentration risk for fee operations. The internal governance of this contract (signer structure, quorum, upgrade authority) was not assessed in this engagement.

BetaDelegateWhitelister: No `BetaDelegateWhitelisterSet` event was observed in the on-chain event history assessed for this report; the address currently holding this role is therefore not confirmed. The owner can override this role at any time. The beta-delegate feature allows whitelisted addresses to execute pre-signed ERC-20 transfers; it cannot mint, pause, or freeze.

ProposedOwner: Zero address (unset). No pending ownership transfer is in progress as of the assessment date.

4.2 Administration History

Role history is complete from deployment (August 2019) through the assessment snapshot (May 2026), sourced from on-chain event data.

Deployment and initial setup (August 2019): The proxy was deployed on 26 August 2019. The proxy admin was changed twice in rapid succession during initial configuration. The supply controller was set and the fee controller was set and adjusted three times in the same block window.

NYDFS approval and initial operations (September 2019): On 5 September 2019, following NYDFS approval, ownership transferred from the deployer EOA to the first operational EOA (`0xb87ce...`). The asset-protection role was set to the same address. The contract became operational under the NYDFS limited purpose trust company charter.

Supply controller rotation (March 2021): The supply controller rotated from `0x5195...` to `0xe25a...`. No incident association; consistent with routine key management.

Major operational reorganisation (May 2021): On 4 May 2021, a significant structural change consolidated all operational roles into the fee controller smart contract (`0x0644bd...`): the proxy admin changed, ownership transferred to the fee controller, the asset-protection role was set to the fee controller, and the fee controller itself was assigned. This represented the highest level of on-chain control sophistication in the system's history, as these key roles were governed by a smart contract rather than bare EOAs.

Supply controller rotation (December 2024): The supply controller rotated from `0xe25a...` to `0x2fb074...` (the current holder). No incident association.

Administrative reorganisation (August 2025): On 7 August 2025, the proxy admin changed to `0xc94bcf...` and the asset-protection role was set to EOA `0x3af3e...`. On 8 August 2025, ownership transferred from the fee controller contract to the same EOA `0x3af3e...`. This reorganisation moved the owner and asset-protection role from a contract-held structure back to EOA control, reducing on-chain governance sophistication for these functions. The timing aligns with the NYDFS $48.5 million settlement (7 August 2025) concerning the BUSD/Binance programme. No PAXG-specific operational rationale for the role-structure change has been publicly documented.

Pause events: No `Pause` or `Unpause` events are present in the assessed history. PAXG has remained unpaused since deployment in 2019.

Upgrade events: No implementation upgrade events have occurred. The current implementation (`0x74271F2282eD7eE35c166122A60c9830354be42a`) has been in place since deployment, over six years without a code change.

Known operational incidents: No operational incidents involving key compromise, freeze misuse, supply manipulation, contract exploit, or emergency intervention have been publicly reported for PAXG. The NYDFS enforcement actions (February 2023 BUSD cessation order; August 2025 $48.5 million settlement) concerned the separate BUSD/Binance stablecoin programme and had no disclosed operational impact on PAXG contracts or key holders.

4.3 Upgrade Risk Analysis

Proxy standard: PAXG uses the `AdminUpgradeabilityProxy` from the ZeppelinOS pre-EIP-1967 era, implementing the transparent proxy pattern. The proxy admin slot is stored at `keccak256("org.zeppelinos.proxy.admin")` (`0x10d6a54a...`) and the implementation slot at `keccak256("org.zeppelinos.proxy.implementation")` (`0x7050c9e0...`). These differ from the EIP-1967 standard slots (`0x360894a1...` and `0xb53127...`). Security tooling, block explorers, and monitoring dashboards that read EIP-1967 slots will not locate the correct implementation or proxy admin addresses. Off-chain systems monitoring for upgrade or admin-change events must explicitly target the ZeppelinOS-specific storage slots to reliably detect such events; standard EIP-1967 watchers will silently miss them.

Upgrade authority and scope: The proxy admin can replace the implementation atomically in a single transaction with no timelock, no second approval, and no advance notice to token holders. `upgradeTo(newImpl)` replaces the implementation slot immediately. `upgradeToAndCall(newImpl, data)` replaces the implementation and then executes an arbitrary call on the proxy. The inner call re-enters the proxy fallback with `msg.sender == proxy address` ; any future initialiser that sets `owner = msg.sender` would set the owner to the proxy address, permanently bricking ownership functions. Future upgrade procedures must pass the intended owner as an explicit constructor or initialiser argument rather than deriving it from `msg.sender` .

No upgrade has occurred in six years of operation.

Storage layout: The implementation uses sequential storage from slot 0. A future implementation that inserts new variables at existing slot positions or changes variable ordering would corrupt stored values. No on-chain storage-layout guard (such as a StorageGap) is present. Storage-layout compatibility is enforced by operational process only, under the issuer's control of both contracts. The proxy's own admin and implementation pointers use unstructured keccak256-derived slots, which avoids collision with the implementation's sequential storage.

Practical risk during upgrade: The upgrade window is effectively instantaneous. If the proxy admin submits an `upgradeTo` transaction, token holders receive no advance notice; a malicious or erroneous implementation takes effect in the same block; and all PAXG balances (approximately $2.262 billion), approvals, freeze states, and role assignments stored in the proxy are immediately subject to the new implementation's logic. Six years of operational stability reduce the likelihood of an upgrade event, but the risk remains material at this asset scale. The absence of a timelock is a design choice made by Paxos; it enables faster emergency patching at the cost of providing no exit window for token holders before any implementation change.

Meridion offers post-upgrade verification scripting as an optional service to confirm deployed-bytecode integrity after each upgrade.

4.4 Recovery Scenarios

SCENARIO 1: OWNER KEY LOST

FIELD	DETAIL
Detection Method	Paxos internal controls only. No on-chain signal distinguishes key loss from key inactivity.
Recovery Possible?	No
Recovery Authority	None. No on-chain succession mechanism exists for the owner role if the current key is permanently inaccessible and no proposedOwner is set.
Recovery Path	No on-chain recovery path. Off-chain legal or regulatory intervention would be required to seek a network-level resolution, which is not a practical path for a production ERC-20.
Prerequisites / Dependencies	Off-chain succession plan (existence and adequacy not publicly verified); internal key management procedures.
Operational Impact	Token cannot be paused in an emergency. AssetProtectionRole, supplyController, feeController, and betaDelegateWhitelister role assignments are permanently frozen. All owner-gated functions become permanently unavailable.
Residual Risk	Permanent loss of emergency pause capability. If a critical implementation vulnerability is discovered, the contract cannot be paused; the proxy admin must perform an upgrade to remediate, adding dependency on proxy admin availability.

SCENARIO 2: SUPPLYCONTROLLER KEY LOST

FIELD	DETAIL
Detection Method	Paxos internal controls. Operationally, inability to process mint or burn requests would surface through normal issuance workflows.
Recovery Possible?	Partial
Recovery Authority	Owner EOA, via `setSupplyController`.
Recovery Path	Owner calls `setSupplyController` with a replacement address. The supply controller can also self-reassign, but that path is unavailable on key loss.
Prerequisites / Dependencies	Owner key availability; prepared replacement supply-controller address and key; off-chain succession plan.
Operational Impact	Mint and burn operations suspended until role is reassigned. New issuance and redemption-linked burns are blocked.
Residual Risk	The replacement key's security posture is unknown until disclosed. If the loss was caused by a systemic infrastructure failure, the replacement may face similar risks.

SCENARIO 3: PROXYADMIN KEY LOST

FIELD	DETAIL
Detection Method	Paxos internal controls only. No on-chain signal. Detected through periodic operational testing of admin functions.
Recovery Possible?	No
Recovery Authority	None. The proxy admin can only be changed by the current admin. No escrow or backup mechanism is visible on-chain.
Recovery Path	No on-chain recovery path. Implementation upgrades become permanently unavailable.
Prerequisites / Dependencies	Off-chain key backup or succession plan (existence not publicly verified).
Operational Impact	Critical vulnerabilities in the implementation cannot be patched. New features cannot be deployed. The token is permanently locked to its current code.
Residual Risk	If a critical vulnerability is discovered post-key-loss, no on-chain remediation path exists. The owner can pause the token but cannot prevent delegatecall-context exploits in the implementation.

SCENARIO 4: PROXYADMIN KEY COMPROMISED

FIELD	DETAIL
Detection Method	On-chain monitoring for `Upgraded` event at the proxy or for storage changes at the ZeppelinOS implementation slot (`0x7050c9e0...`). Monitoring targeting EIP-1967 slots (`0x360894...`) will silently miss the event. Real-time detection is critical; no timelock provides any response window.
Recovery Possible?	Partial
Recovery Authority	Owner EOA (partial mitigation only: can pause token; cannot reverse an upgrade).
Recovery Path	If detected before the attacker acts on the hostile implementation: owner can pause the token to halt transfers and wipe operations. No on-chain mechanism exists to roll back an implementation upgrade. Full recovery requires recovering proxy admin control through off-chain means.
Prerequisites / Dependencies	Real-time monitoring correctly configured for ZeppelinOS storage slots; owner key availability and response speed; ability to recover or block the compromised proxy admin key off-chain.
Operational Impact	Implementation replaced immediately in the compromising transaction. If hostile: all PAXG balances (approximately $2.262 billion) potentially accessible via delegatecall-manipulated storage.
Residual Risk	If a hostile implementation was deployed and acted upon before detection, user balances may be irrecoverable on-chain. The ZeppelinOS monitoring blind spot increases time-to-detection. No on-chain rollback exists.

SCENARIO 5: SUPPLYCONTROLLER KEY COMPROMISED

FIELD	DETAIL
Detection Method	On-chain monitoring for `SupplyIncreased` events at unusual magnitudes or frequencies. Standard ERC-20 Transfer events from the zero address would also appear in transfer logs.
Recovery Possible?	Partial
Recovery Authority	Owner EOA, via `setSupplyController` and `pause`.
Recovery Path	Owner rotates the supply controller role as quickly as possible. Owner may also pause the token to prevent distribution of fraudulently minted tokens. Tokens minted before rotation cannot be reversed on-chain; no burn-without-consent function is available to the owner.
Prerequisites / Dependencies	Owner key availability and rapid response; prepared replacement supply-controller address; real-time monitoring for `SupplyIncreased` events.
Operational Impact	Unlimited PAXG minting until role is rotated. Fraudulently minted tokens may be rapidly distributed to exchanges or DeFi protocols.
Residual Risk	Minted tokens distributed before role rotation are not recoverable. Depending on the scale of minting, this could cause permanent supply inflation and gold-backing ratio impairment.

SCENARIO 6: ACCIDENTAL OR MALICIOUS TOKEN PAUSE

FIELD	DETAIL
Detection Method	Immediate and universal: all PAXG transfer, approve, and betaDelegatedTransfer calls revert. DeFi integrations, exchanges, and direct users observe failures instantly.
Recovery Possible?	Yes
Recovery Authority	Owner EOA, via `unpause()`.
Recovery Path	Owner calls `unpause()` in a single transaction. No secondary approval or waiting period is required.
Prerequisites / Dependencies	Owner key availability; determination that the pause was accidental or that the triggering incident is resolved.
Operational Impact	All PAXG transfers globally halted for the duration of the pause. DeFi collateral positions using PAXG may be unable to be liquidated or adjusted. Exchange withdrawals and deposits blocked.
Residual Risk	None operationally if corrected promptly. Reputational and DeFi-integration risk if pause is prolonged or unexplained.

The recovery design for PAXG is highly centralised. The proxy admin and owner roles have no on-chain successor mechanism: permanent key loss permanently eliminates the corresponding privilege. The supply controller has a partial recovery path through the owner. All recovery paths ultimately depend on off-chain

operational continuity plans that are not publicly documented. Paxos's SOC 2 Type 2 certification (obtained March 2021, renewal status not public) indicated that internal controls were audited at that time, but the scope and adequacy of those controls for the specific recovery scenarios above is not externally verifiable.

4.5 Multisig Security Analysis

No multisig role holder was identified for any PAXG privileged role as of the assessment date. On-chain code verification confirms that the proxy admin (`0xc94bcf6e1d8b3558e3b62e743630d50497e3851c`) is a bare externally owned account with no deployed bytecode, providing no on-chain governance mediation for the highest-privilege role in the system. The owner (`0x3af3e85f4f97de7ad0f000b724fb77fe5ffc024b`) and supply controller (`0x2fb074fa59c9294c71246825c1c9a0c7782d41a4`) are similarly confirmed bare EOAs. All three roles for which multisig analysis was performed are confirmed single-key accounts with no threshold protection. The fee controller (`0x0644bd0248d5f89e4f6e845a91d15c23591e5d33`) is a contract, and its internal governance structure — including signer arrangement, quorum, and upgrade authority — was not assessed in this engagement.

---

5. Part III: Financial Analysis

Financial Risk Rating: Low | Confidence: Medium

5.1 Underlying Asset Attestation

PAX Gold (PAXG) is backed 1:1 by physical gold held in LBMA-approved vaults in London. Each PAXG token represents exactly one fine troy ounce of an LBMA Good Delivery gold bar. Paxos publishes monthly attestation reports at the Paxos transparency page.

Attestation programme: KPMG LLP, monthly AICPA examination-level attestation.

Most recent attestation report: April 2026 (KPMG LLP, available on the Paxos transparency page).

METRIC	VALUE	SOURCE
On-chain PAXG total supply (snapshot)	479,162.743 PAXG	`eth_call totalSupply()` on-chain at block 25042795
Required gold backing (structural)	479,162.743 fine troy oz	By design (1 PAXG = 1 oz); structurally derived
USD value of required gold	$2,262,136,893	Market price $4,721.02/oz x on-chain supply
Market-reported circulating supply	471,942.854 PAXG	CoinGecko API
CoinGecko market cap	$2,228,044,038	CoinGecko API
Implied collateralisation ratio (USD basis)	101.53%	On-chain supply x spot price / CoinGecko market cap
Market price	$4,721.02 / oz	Market (assessment snapshot date)
24-hour reported volume (CEX)	$198,976,987	Aggregated across 30 venues
24-hour reported volume (DEX, main pools)	approx. $8.1M	DeFiLlama and on-chain pool data

The on-chain `totalSupply` (479,162.743 PAXG) exceeds the CoinGecko circulating supply (471,942.854 PAXG) by 7,219.889 PAXG (~1.53%). This discrepancy is consistent with Paxos holding treasury tokens: minted PAXG backed by physical gold but not yet distributed into the secondary market. Treasury tokens are included in `totalSupply` but excluded from CoinGecko's circulating supply definition. No reserve shortfall is implied; treasury tokens require corresponding gold in custody.

Gold is held in allocated, segregated accounts at two LBMA-accredited London vaults: Brink's Global Services Ltd. and ICBC Standard Bank Plc. The allocation split between these two custodians is not publicly disclosed. Paxos provides a real-time gold allocation lookup tool listing each bar by serial number and weight.

The April 2026 KPMG AICPA examination report was confirmed available on the Paxos transparency page at assessment time. The on-chain `totalSupply` and the structural 1:1 oz design were used as the reserve basis for this assessment.

5.2 Counterparty Risk Profile

PARTY	ROLE	JURISDICTION	RISK SUMMARY
Paxos Trust Company, LLC	Issuer / operator / redemption processor	United States (NYDFS trust company; conditional OCC conversion approval)	Low-medium credit risk; strong regulatory standing; no PAXG-specific enforcement history.
KPMG LLP	Monthly attestor (AICPA examination)	United States (Big Four)	Very low credit and reputational risk; reliance on custodian representations for bar-level verification.
Brink's Global Services Ltd.	Physical gold custodian (LBMA vault 1)	United Kingdom / United States	Low credit risk; global leader in physical security; allocated gold is legally segregated under UK law.
ICBC Standard Bank Plc	Physical gold custodian (LBMA vault 2)	United Kingdom	Low-medium credit risk; LBMA member; allocated gold segregated; standalone credit rating not publicly available.

Paxos Trust Company, LLC: Paxos is the issuer, supply controller, redemption processor, and regulatory compliance obligor for PAXG. It was originally incorporated in New York State as a limited purpose trust company and received NYDFS approval for PAXG on 5 September 2019. On 12 December 2025, the OCC conditionally approved Paxos's application to convert to a national trust bank, subject to satisfying OCC conditions. Final completed conversion was not independently confirmed during this assessment, so this report does not treat PAXG as already operating under a completed OCC charter. Paxos raised $300 million in a Series D round in 2021 and has operated since 2012. The 2023 BUSD cessation order and the August 2025 $48.5 million NYDFS civil monetary penalty both relate exclusively to the BUSD/Binance stablecoin partnership and have no disclosed impact on PAXG operations, contracts, or key holders. The principal risk is single-issuer concentration: PAXG has no decentralised governance or alternative redemption path if Paxos operations are suspended. Paxos public materials state that PAXG customers own the underlying physical gold represented by the token; however, the public legal documentation reviewed here does not clearly establish how an individual holder would directly enforce a property claim to specific bars in insolvency, as distinct from contractual redemption rights against Paxos. Recovery would therefore depend on trust-law treatment, custody documentation, and applicable regulatory proceedings.

KPMG LLP: KPMG is one of the largest global accounting firms and was appointed as PAXG attestor from 28 February 2026, replacing WithumSmith+Brown, PC. Attestations are conducted under AICPA examination-level standards, which are more rigorous than agreed-upon procedures. KPMG's engagement relies on physical inspection and bar-list confirmation provided by the custodians; the examination does not constitute a bar-by-bar purity assay. Attestation lag is inherent to monthly reporting: up to 30 days of unattested period exist between report dates. KPMG's credit and reputational risk are very low for this engagement scope.

Brink's Global Services Ltd.: Brink's is the world's largest physical security and logistics company, with over 165 years of operating history and a NYSE listing (BCO). It operates LBMA-accredited vaults in London. Gold held in allocated accounts at Brink's is legally segregated from Brink's general assets under UK law and

LBMA Rules. In an insolvency, allocated gold belongs to the beneficial owner (Paxos, for the benefit of PAXG holders) and is not available to general creditors. Brink's maintains insurance against physical loss of gold in custody, though coverage scope is not publicly disclosed. Credit risk is low.

ICBC Standard Bank Plc: ICBC Standard Bank is a UK-regulated bank and LBMA member, jointly owned by the Industrial and Commercial Bank of China Ltd. (ICBC) and Standard Bank Group. ICBC is the world's largest bank by assets. Allocated gold held at ICBC Standard Bank is legally segregated under UK law and LBMA Rules, providing similar bankruptcy remoteness to the Brink's arrangement. ICBC Standard Bank Plc does not carry a publicly available standalone credit rating, and its financial strength depends on parent support from ICBC. Exposure to Chinese parent-company risk and regulatory developments affecting ICBC are secondary considerations. The undisclosed allocation split between Brink's and ICBC Standard Bank prevents precise custodian concentration assessment; if one custodian holds the majority of gold, a single-custodian failure scenario is materially worse than the 50/50 assumption used in scenario modelling.

5.3 Liquidity Risks and Scenario Analysis

5.3.1 LIQUIDITY PROFILE

Issuer redemption process: Direct creation and redemption of PAXG through Paxos requires passing Paxos KYC and AML onboarding. Physical gold delivery (London Good Delivery bars) requires a minimum of 430 PAXG (one full bar) with T+2 settlement during LBMA business hours. USD cash redemption is available at lower thresholds (exact minimum not published) at prevailing LBMA spot prices, settled via bank wire. Redemption fees are tiered, ranging from 0.03% to 1%. Transfer fees were set to zero in July 2024. Banking-hours dependencies apply to USD settlement. Holders with fewer than 430 PAXG cannot redeem for physical gold directly through Paxos.

DEX liquidity: Total reported DEX TVL (deduplicated) is approximately $192 million. Conservative executable DEX liquidity is approximately $55.7 million after excluding a $124.98 million restricted institutional pool (multipli.fi) and lending pools (Fluid, Morpho Blue; combined approximately $7.8 million) that are not executable for ordinary holders.

VENUE	TYPE	TVL (USD)	NOTES
PAXG-WETH (Uniswap V2)	DEX	$15,865,995	24h volume $440,752
PAXG-XAUT (Uniswap V3, 0.01%)	DEX	$9,343,946	24h volume $5,189,237; gold-for-gold swap
PAXG-XAUT (Uniswap V4, 0.05%)	DEX	$6,680,194	Gold-for-gold swap; no direct USD exit
PAXG-USDC (Uniswap V3, 0.05%)	DEX	$3,273,177	24h volume $2,141,198
PAXG-XAUT (Uniswap V3, 0.05%)	DEX	$4,190,643	Gold-for-gold swap
PAXG-XAUT (Fluid DEX)	DEX	$4,091,539	24h volume $151,058; gold-for-gold swap
multipli.fi restricted pool	DEX (restricted)	$124,975,573	Institutional/restricted; excluded from executable depth
Fluid Lending, Morpho Blue	Lending	approx. $7,800,000	Collateral pools; excluded from executable depth
Binance (PAXG/USDT)	CEX	24h vol. $34,680,982	Reported turnover
Coinbase Exchange (PAXG/USD)	CEX	24h vol. $2,466,233	Reported turnover
Kraken (PAXG/EUR)	CEX	24h vol. $2,030,750	Reported turnover
Gemini (PAXG/USD)	CEX	24h vol. $2,284,746	Reported turnover
OKX (PAXG/USDT)	CEX	24h vol. $3,165,172	Reported turnover

PAXG-XAUT pools provide gold-for-gold swaps and offer no direct USD exit without routing XAUT proceeds to a USDC or USDT pair separately. The conservative executable DEX liquidity of $55.7 million represents approximately 2.46% of the on-chain reserve value of $2.262 billion. On a consistent cross-report basis, this is the strongest DEX liquidity coverage among the three reviewed gold-token reports, ahead of XAUT's approximately 1.7% reserve-value coverage and PGOLD's approximately 0.41% market-cap coverage. For positions above approximately $10 million, direct issuer redemption (T+2) or OTC and CEX desks are necessary. Mass-exit scenarios beyond $55.7 million in DEX depth within a 6-hour window will result in material secondary-market discounts.

5.3.2 SCENARIO ANALYSIS

Scenario 1: Base Case

FIELD	DETAIL
Trigger Conditions	Normal operating environment; redemption demand within historical norms (approximately 1% of supply per day, or about 4,792 PAXG at $4,721.02 per oz, totalling approximately $22.6 million); collateral fully attested and gold price stable.
Effect on Collateral	1:1 oz backing maintained; USD reserve value unchanged at approximately $2.262 billion. No collateral stress.
Liquidity Runway	Conservative executable DEX depth of $55.7 million comfortably absorbs normal daily flow. Paxos USD redemption channels handle remaining demand. No DEX exhaustion risk.
Anticipated Investor Actions	Normal secondary-market activity; small redemptions via Paxos direct channels; DeFi utilisation at normal levels.
Conclusion	Fully solvent and operational. No liquidity or reserve concerns under base conditions.
Impact	Low

Scenario 2: Market Stress

FIELD	DETAIL
Trigger Conditions	Gold price declines 20% from $4,721.02 to $3,776.82 per oz, driven by a macroeconomic event or broad commodity selloff.
Effect on Collateral	PAXG remains 1:1 backed in oz terms throughout; reserve insolvency cannot occur from a gold price movement. USD value of reserves declines to approximately $1.810 billion. USD-denominated holders experience mark-to-market losses and some accelerate redemption or DEX selling.
Liquidity Runway	Modelled elevated demand: 5% of on-chain supply seeking USD exit (approximately $90.5 million at the new price). DEX depth ($55.7 million) is fully consumed; approximately $34.8 million flows to CEX and direct issuer redemption (T+2).
Anticipated Investor Actions	Elevated selling pressure; retail holders exit via DEX; institutional holders use CEX or direct redemption. Some holders retain PAXG as gold exposure at reduced USD cost basis.
Conclusion	Solvent and operational throughout. Secondary-market discount of approximately 1-2% likely during peak stress as DEX depth exhausts. PAXG's gold-price peg means USD losses are a feature of the asset's commodity exposure, not a structural failure.
Impact	Medium

Scenario 3: Redemption Run / Mass Exit

FIELD	DETAIL
Trigger Conditions	A confidence shock triggers coordinated exit of 25% of circulating supply (approximately 119,791 PAXG, approximately $565.5 million at spot) within 6 hours.
Effect on Collateral	Reserves remain fully gold-backed (1:1 oz) throughout. USD reserve value declines only by the gold redeemed. No insolvency; the protocol is solvent but access is gated by settlement infrastructure.
Liquidity Runway	DEX depth ($55.7 million) is exhausted within approximately the first hour. Remaining approximately $509.8 million requires CEX order book depth or direct issuer redemption queues. Physical bar delivery (T+2; 430 oz minimum) and USD redemption (banking hours; Paxos processing capacity) create hard capacity constraints. A 6-hour window cannot absorb $565 million in aggregate.
Anticipated Investor Actions	Rapid selling on all available DEX and CEX venues; direct Paxos redemption queue build-up; secondary-market discount of 5-10% emerges as DEX liquidity depletes. Holders with fewer than 430 PAXG cannot access direct physical redemption and must accept secondary-market prices.
Conclusion	Solvent but gated. The protocol remains fully gold-backed; the constraint is redemption infrastructure capacity, not solvency. Secondary-market discounts are the primary harm mechanism.
Impact	High

Scenario 4: Oracle Failure / Price-Source Failure

FIELD	DETAIL
Trigger Conditions	The primary on-chain gold price oracle (Chainlink XAU/USD) becomes unavailable or stale for 15 minutes or longer, affecting DeFi protocols that use PAXG as collateral.
Effect on Collateral	PAXG's core ERC-20 functions (mint, burn, transfer) have no on-chain oracle dependency. Paxos uses LBMA published gold-fix prices for direct USD redemptions, independent of Chainlink. Collateral valuation in DeFi lending protocols (Morpho Blue approximately $0.8 million TVL; Fluid Lending approximately $7 million TVL) may be frozen during the outage.
Liquidity Runway	Modelled demand: 2% of on-chain supply exiting via DEX as DeFi users unwind PAXG-collateralised positions (approximately $45.3 million). DEX conservative depth ($55.7 million) can absorb this demand. Secondary DEX markets continue price discovery independent of Chainlink.
Anticipated Investor Actions	DeFi users manually unwind collateral positions; oracle-dependent protocols pause new borrows or liquidations; direct holders unaffected.
Conclusion	Solvent and operational. Impact limited to temporary DeFi integration disruption. Recovery typically occurs within 1-2 hours as Chainlink restores the feed or falls back to alternative sources.
Impact	Medium

Scenario 5: Custodian Failure

FIELD	DETAIL
Trigger Conditions	One of the two London custodians (Brink's Global Services Ltd. or ICBC Standard Bank Plc) is unable to process vault operations or gold deliveries for 48 hours or more due to operational failure, regulatory action, or insolvency proceedings.
Effect on Collateral	Gold held in LBMA allocated accounts is legally segregated from the custodian's general estate under UK law and LBMA Rules; gold ownership is not at risk. However, logistical access to gold held at the suspended custodian is unavailable. With the allocation split undisclosed, the proportion accessible via the operating custodian is uncertain; modelling assumes approximately 50% accessibility.
Liquidity Runway	Modelled demand: 10% of supply seeking redemption within 48 hours (approximately 47,916 PAXG, approximately $226.3 million). Physical delivery suspended for bars at the suspended custodian; USD redemption available only for gold held at the operating custodian. DEX and CEX secondary markets remain open throughout. Secondary-market discount of 2-4% develops within 24 hours, widening to 5-8% if the suspension extends beyond 5 business days.
Anticipated Investor Actions	Secondary-market selling accelerates as news spreads; institutional holders queue for direct redemption from accessible custodian; Paxos initiates legal and operational gold-transfer procedures.
Conclusion	Solvent but gated. Gold is legally secure; the risk is operational and logistical. Dual-custodian structure limits severity relative to a single-custodian model. Paxos would need to initiate gold transfer to an alternative LBMA vault, typically 5-10 business days under normal circumstances. The undisclosed allocation split is the primary uncertainty in this scenario.
Impact	High

5.4 Regulatory and Legal Jurisdiction

Issuer jurisdiction: United States (NYDFS New York state trust company; conditional OCC national trust bank conversion approval)

Governing law: New York State law

REGULATORY ITEM	DETAIL
Primary regulator	NYDFS; OCC conditional conversion approval dated 12 December 2025
Licence / registration	NYDFS limited purpose trust company charter; OCC national trust bank conversion conditionally approved, final completed conversion not independently confirmed in this assessment
AML / KYC framework	Bank Secrecy Act (BSA) as administered by FinCEN; NYDFS AML/CFT requirements; OCC requirements would apply upon completed conversion
Enforcement history	No actions against PAXG specifically. NYDFS: February 2023 BUSD minting cessation order; August 2025 $48.5 million civil monetary penalty. Both relate exclusively to the BUSD/Binance programme.
Pending proceedings	None identified as of assessment date.

Paxos Trust Company, LLC operates under a strong US state trust-company framework and received conditional OCC approval on 12 December 2025 to convert to a national trust bank. A completed OCC national trust bank charter would bring Paxos under federal banking supervision, including regular safety-and-soundness examinations, capital adequacy requirements, and consumer protection rules; however, final completed conversion was not independently confirmed during this assessment. PAXG was the first gold-backed token approved by NYDFS (September 2019).

Paxos publicly represents that PAXG customers own the underlying physical gold represented by their tokens. The public-facing documentation reviewed in this assessment nevertheless does not clearly establish the mechanism by which an individual token holder could directly assert a property interest in specific gold bars in an insolvency scenario, as distinct from enforcing contractual redemption rights against Paxos Trust Company, LLC for physical gold (minimum 430 PAXG per bar) or USD cash at prevailing LBMA prices. Gold is held in allocated, segregated accounts under New York trust-law arrangements, which should support bankruptcy remoteness from Paxos's general corporate estate, but the individual holder enforcement path remains a meaningful legal uncertainty.

PAXG faces an active regulatory gap in the European Union. As a gold-referenced token, PAXG falls under the EU Markets in Crypto-Assets Regulation (MiCA) as an Asset-Referenced Token (ART). Paxos has not announced a MiCA ART authorisation from an EU competent authority as of this assessment date. EU-based crypto-asset service providers (CASPs) and retail investors may face restrictions on offering or holding PAXG without a MiCA-authorised issuer or an applicable exemption. This gap presents a material distribution risk for EU market access and may affect PAXG's competitiveness relative to EU-licensed gold-token alternatives. Paxos has not published UK-specific regulatory authorisation either, though the UK's emerging crypto-asset regulatory framework remains less prescriptive than MiCA at this stage.

The regulatory environment for tokenised commodities is improving globally, with the OCC conditional conversion approval being a significant positive development for Paxos if the conversion is completed. US stablecoin legislation, if enacted, may clarify or affect the treatment of commodity-backed tokens. PAXG's commodity classification (gold) is stable under current US law, though future legislative or regulatory interpretive changes by the SEC or CFTC could affect this characterisation.

6. Conclusion

6.1 Composite Risk Rating: Low

Composite Confidence: Low

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

PAX Gold (PAXG) receives a composite risk rating of **Low** under the Meridion Risk Rating Standard v1. The rating reflects one domain at Medium (operational security) under conditions that are contingent and not currently causing holder harm: the proxy admin, owner and asset-protection role, and supply controller are all confirmed bare externally owned accounts controlling approximately $2.262 billion in token value, operating without on-chain timelocks, second-approval requirements, or publicly disclosed key management controls. No operational incident involving key compromise, unauthorised minting, or misuse of administrative authority has been recorded in six years of operation. The smart contract domain is rated Low; the deployed code presents only a single Low-severity event-log finding (SEC-01), formal verification confirmed the complete absence of hidden-surface trapdoors in the deployed bytecode, and six years of uninterrupted operation on an unchanged implementation support the Low rating. The financial domain is rated Low; the 1:1 gold-oz backing eliminates fractional-reserve risk, monthly KPMG AICPA attestations provide independent reserve confirmation, and Paxos's conditional OCC conversion approval is a positive regulatory development, though not treated here as completed OCC charter status.

Composite confidence is **Low**, driven by the absence of publicly disclosed key management evidence for the three confirmed highest-privilege EOA roles (proxy admin, owner, and supply controller). The undisclosed custodian allocation split between the two London vaults further prevents the composite confidence from reaching Medium. The smart contract domain achieves High confidence following the completion of formal verification and all 57 fork-based behavioral tests.

6.2 Improvement Suggestions

- **Transparency of operational security practices:** Paxos has not publicly disclosed the key management policy, recovery and incident-response procedures, or operational monitoring policies for the PAXG privileged roles. Specifically: (a) key management policy should disclose whether HSM, MPC, or equivalent hardware security controls are used for the proxy admin, owner, and supply-controller keys, and the key ceremony and rotation schedule; (b) the recovery and incident-response playbook should address key loss, key compromise, and emergency pause scenarios for each privileged role, including succession procedures for the proxy admin and owner; (c) the monitoring policy should describe the on-chain event thresholds and alert configurations used for `Upgraded`, `SupplyIncreased`, `AddressFrozen`, `FrozenAddressWiped`, and `OwnershipTransferred` events, noting the requirement to

monitor ZeppelinOS-specific storage slots rather than EIP-1967 slots for upgrade detection. Publishing these disclosures would allow external verifiers to assess whether the operational posture matches the asset's scale and regulatory standing.

- **Disclose the gold allocation split between custodians:** The proportion of PAXG gold reserves held at Brink's Global Services Ltd. versus ICBC Standard Bank Plc is not publicly disclosed. Disclosure would enable holders and analysts to assess custodian concentration risk and validate the assumptions used in the custodian-failure scenario analysis.
- **Pursue MiCA authorisation for EU market access:** PAXG is classifiable as an Asset-Referenced Token under MiCA. Paxos has not announced a MiCA ART authorisation as of this assessment date. Pursuing authorisation from an EU competent authority would eliminate the EU distribution risk for PAXG and support institutional adoption in European markets.

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 either the AdminUpgradeabilityProxy or PAXGImplementation
- A change to any privileged role holder identified in section 4.1
- A material change to the custodian arrangement, redemption model, attestor, or reserve composition identified in sections 5.1 and 5.4
- 12 months from the date of publication
