AUGR Risk Reclassification Dossier

Governance Hardening, Risk Context, and Verification Packet

Auronex

May 26, 2026

1 Executive Summary

AUGR on BNB Smart Chain can be flagged as high risk by generic scanners because it is upgradeable and has privileged controls. This dossier provides a focused evidence package for governance posture, role topology, and verifier procedure used in risk reclassification reviews by exchanges, data aggregators, and third-party monitors.

2 Scope and Objective

Objective: request reclassification from generic "high risk" labeling to a governance-aware classification that reflects current operational controls.

Scope:

- AUGR proxy and implementation architecture,
- timelock and role-holder governance model,
- operational privilege boundaries,
- public verification workflow and artifacts.

3 Token Identity

- Token name: Auronex Gold
- Ticker: AUGR
- Network: BNB Smart Chain (Chain ID 56)
- Token proxy address: `0xeD6eAe940e7b9B1C92dC6bD9BF9690AA7E753ACc`

4 Current External Risk Labels

- Contract upgradeable
- Privileged role surface present
- Scanner-driven high-risk heuristics

Upgradeable status alone is not equivalent to malicious behavior; risk should be assessed against live role authority and governance controls.

5 Root Cause of High-Risk Classification

Common scanner heuristics that trigger high-risk classification:

1. Upgradeability is detected.
2. Privileged authority appears concentrated or unclear.
3. Incomplete machine-readable governance disclosure.
4. Limited public artifacts proving operational constraints.

6 Governance and Security Control Model

- AUGR remains on the existing proxy address (no migration event required).
- Upgrade authority is delegated to dedicated timelock governance.
- Operational privileged roles are held by operations safe, separated from upgrader control.
- Governance state is tracked in deployment manifest and public runbooks.

7 Technical Mitigation Package

Repository utilities (mainnet):

- `apps/anx-contracts/scripts/propose-align-augr-role-topology.ts`
- `apps/anx-contracts/scripts/check-augr-role-topology.ts`

- `apps/anx-contracts/scripts/deploy-augr-timelock-controller.ts`
- `apps/anx-contracts/scripts/verify-augr-timelock-controller.ts`

Finalized role topology intent:

- `UPGRADER_ROLE` on dedicated AUGR timelock.
- `PAUSER_ROLE`, `BLOCKER_ROLE`, `CONFISCATION_ROLE`, `MINTER_ROLE`, `ADMIN_BURN_ROLE` on operations safe.

8 Reviewer Verification Procedure

Reviewers can verify:

1. AUGR proxy address continuity.
2. Timelock proposer/executor/admin ownership by governance safe.
3. `UPGRADER_ROLE` moved to new AUGR timelock and removed from prior timelock.
4. Operational privileged roles remain on operations safe.
5. Proxy and timelock deployments are verified and auditable.

9 Evidence Checklist (Populated)

1. AUGR proxy (BscScan): `https://bscscan.com/address/0xeD6eAe940e7b9B1C92dC6bD9BF9690AA7E753ACc`
2. AUGR timelock (BscScan): `https://bscscan.com/address/0x0D6a54ed869b02dA15148be4044952cDE82CA73b`
3. Timelock code (BscScan): `https://api.bscscan.com/api/address/0x0D6a54ed869b02dA15148be4044952cDE82CA73b#code`
4. Governance safe (BscScan): `https://bscscan.com/address/0xdB12be621612d15E7514D196548F655735AaDe7a`
5. Operations safe (BscScan): `https://bscscan.com/address/0x9A7059CcFC3d36E32bceF9a1eaca80f22f6fb857`
6. Executed upgrader-rotation Safe tx hash: `0x0a413bde...f6e4a958` (full hash in manifest and Safe queue records)
7. AUGR governance trust framework: `https://github.com/Auronex-DAO/contracts/blob/main/docs/augr-governance-trust-framework.md`
8. AUGR timelock runbook: `https://github.com/Auronex-DAO/contracts/blob/main/docs/augr-timelock-upgrade-runbook.md`

10 Canonical Submission Statement

AUGR uses an upgradeable architecture with explicit governance hardening. Upgrade authority is timelock-bound, operational privileged roles are separated onto operations safe, and all privileged transitions are publicly auditable. No proxy-address migration or holder migration was required to enforce the governance model.

11 Residual Risk Disclosure

Residual risks include multisig signer compromise, governance process failures, and monitoring/response lag. Current posture mitigates these through role separation, timelock delay, strict preflight checks, and public evidence artifacts.

12 Planned Hardening Roadmap

1. **Completed (May 26, 2026):** Dedicated AUGR timelock deployed and verified at `0x0D6a54ed869b02dA15148be4044952cDE82CA73b`.
2. **Completed (May 26, 2026):** AUGR `UPGRADER_ROLE` rotated from prior timelock to new timelock via Safe proposal `0x0a413bde...f6e4a958`.
3. Continue periodic governance-role attestation snapshots and incident-response drills.
4. Continue external reviewer tooling improvements for machine-readable governance proofs.

13 Contact and Disclosure

- Project: Auronex
- Security contact: hello@auronex.app
- Technical contact: hello@auronex.app
- Disclosure channel: `https://github.com/Auronex-DAO/contracts/issues`