



ANX Risk Reclassification Dossier

Governance Hardening, Risk Context, and Verification Packet

Auronex

May 26, 2026

1 Executive Summary

ANX on BNB Smart Chain has been flagged as high risk primarily due to upgradeable-contract architecture and third-party risk labeling. This dossier provides a full evidence package, governance disclosures, and technical verification checklist for risk reclassification reviews by scanners, exchanges, and data aggregators.

2 Scope and Objective

Objective: request reclassification from generic “high risk” treatment to a governance-aware classification that reflects current upgrade/admin controls.

Scope:

- ANX proxy and implementation architecture,
- privilege model and role governance,
- operational controls,
- evidence and verifier workflow.



3 Token Identity

- Token name: Auronex
- Ticker: ANX
- Network: BNB Smart Chain (Chain ID 56)
- Token proxy address: 0xc3ab9c26bc44776f3fc770afd90a27cfb826965c

4 Current External Risk Labels

- Contract upgradeable
- Risk flagged by third-party platforms

Upgradeable status alone is not equivalent to malicious intent; primary risk hinges on upgrade authority design, controls, and auditability.

5 Root Cause of High-Risk Classification

Common scanner heuristics driving high-risk classification:

1. Upgradeability present.
2. Privileged role concentration (single EOA or opaque governance).
3. Incomplete or unclear verification/disclosure artifacts.
4. Weak machine-readable signals for governance constraints.

6 Governance and Security Control Model

- ANX uses an upgradeable proxy architecture.
- Administrative and upgrade privileges are migrated from single-key operation to multisig governance flow.
- Role governance intent: least privilege, explicit boundaries, public auditable role holders.

7 Technical Mitigation Package

Repository utility (mainnet):

- Script: `apps/anx-contracts/scripts/propose-proxy-risk-mitigation.ts`
- Entrypoint: `propose-proxy-risk-mitigation:mainnet`

Action sequence per proxy:



1. `grantRole(DEFAULT_ADMIN_ROLE, ADMIN_MULTISIG)`
2. `grantRole(UPGRADER_ROLE, ADMIN_MULTISIG)`
3. `revokeRole(UPGRADER_ROLE, DEPLOYER_ADDRESS)`
4. `revokeRole(DEFAULT_ADMIN_ROLE, DEPLOYER_ADDRESS)`

Invariant:

- no token proxy address change,
- no holder migration,
- no balance migration.

8 Reviewer Verification Procedure

Reviewers can verify:

1. ANX proxy address continuity.
2. `DEFAULT_ADMIN_ROLE` holder is multisig.
3. `UPGRADER_ROLE` holder is multisig.
4. prior EOA no longer holds those roles.
5. proxy and implementation contracts are verified.
6. role migration transactions are auditable.

9 Evidence Checklist (Populated)

1. ANX proxy (BscScan): <https://bscscan.com/address/0xc3ab9c26bc44776f3fc770afd90a27cfb826965c>
2. ANX implementation (BscScan): <https://bscscan.com/address/0x99f152f899ae95a99f0d5cd21fd9786633198b76>
3. Admin multisig (BscScan): <https://bscscan.com/address/0x9A7059CcFC3d36E32bceF9a1eaca80f22f6fb857>
4. Admin multisig queue (Safe): <https://app.safe.global/transactions/queue?safe=bnb:0x9A7059CcFC3d36E32bceF9a1eaca80f22f6fb857>
5. Governance/process runbook: <https://github.com/Auronex-DAO/contracts/blob/main/docs/proxy-risk-mitigation.md>
6. Security documentation: <https://github.com/Auronex-DAO/contracts/blob/main/apps/anx-contracts/SECURITY.md>
7. Public risk/trust disclosure dossier: <https://github.com/Auronex-DAO/contracts/blob/main/docs/anx-risk-reclassification-packet.md>



10 Canonical Submission Statement

ANX uses an upgradeable architecture with governance hardening controls. Upgrade/admin rights are handled through multisig governance instead of single-key authority. Contract verification and role migration actions are publicly auditable. The ANX proxy address remains unchanged, and no holder migration is required. Reclassification is requested based on current control architecture and verifiable governance evidence.

11 Residual Risk Disclosure

Residual risks include multisig signer compromise risk, process failure risk, and monitoring/response lag risk. Current mitigation posture is least privilege, operational security for signers, and public auditability of privileged actions.

12 Planned Hardening Roadmap

1. **Completed (2026-05-26):** Formal timelock enforcement is active for ANX upgrade path (configured delay: 48 hours / 172800 seconds; ANX UPGRADER_ROLE currently held by timelock 0xea2DaC238Dd9959f2290309441964Fb86E41d87c).
2. Continue role minimization.
3. Expand governance attestation artifacts.
4. Periodic external security review of governance/upgrade workflows.

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>