

STATE MIND


Dual Governance escrow fix review and deployment validation

18-08-2025 – 19-08-2025



1. Project brief	2
2. Conclusion	4

1. Project brief



Title	Description
Client	Lido
Project name	Dual Governance escrow fix review and deployment validation
Timeline	18-08-2025 - 19-08-2025

Project Log

Date	Commit Hash	Note
18-08-2025	8c77d57a4c415bb69c6873d174be7c30b1103907	Commit for DG updated contracts and service contracts

Short Overview

Lido has requested Statemind to review the fix of their Dual Governance contracts and to validate the deployment and service contracts.

The purpose of the validation is to ensure that deployed contracts' sources match the audited commit and has the proper parameters. A fix review verifies that the issue has been resolved correctly and that the implementation is sound. Review of service contracts involves verifying their logic and ensuring the correctness of vote construction and Dual Governance state verification.

The validation consists of two main parts:

- Dual Governance contracts: [dual-governance/contracts](#)
- Sevice contracts [dual-governance/scripts/escrow-upgrade](#)

Reference commits and audit reports

Repository	Commit	Audit Report	Type
dual-governance	3e0f1ae5740ef8410e928f6cc106e3a5f45a5a75	2025-02-05	Audit
dual-governance	7480c3cdc813312c0c36d6faf0f7e6e4148ebfb2*	2025-06-05	Deployment

Notes

* – As part of the upgrade plan, only a subset of contracts was redeployed. In the new deployment commit 8c77d57a4c415bb69c6873d174be7c30b1103907 only the Escrow.sol contract’s code was changed; the other contracts have



































not changed since the previous deployment commit.

Accordingly, the, DualGovernance.sol, TiebreakerCoreCommittee.sol, TiebreakerSubCommittee.sol contracts were redeployed, but their code was untouched and their bytecode is identical to the audited version. The updated Escrow.sol code has been reviewed. The composition of the Tiebreaker Sub-Committees remains the same. All other deployed contracts remain current.

Additional ImmutableDualGovernanceConfigProvider.sol was deployed for legacy contracts to prevent entry into a vulnerable state and allow users to freely withdraw funds from the old Escrow.sol.

Project Scope

The audit covered the following files:

 Escrow.sol	 AssetsAccounting.sol	 DualGovernance.sol
 DualGovernanceStateTransitions.sol	 EmergencyProtectedTimelock.sol	 HashConsensus.sol
 ExecutableProposals.sol	 DualGovernanceStateMachine.sol	 WithdrawalsBatchesQueue.sol
 Tiebreaker.sol	 EmergencyProtection.sol	 DualGovernanceConfig.sol
 EscrowState.sol	 Proposers.sol	 TiebreakerCoreCommittee.sol
 TiebreakerSubCommittee.sol	 Duration.sol	 TimelockState.sol
 EnumerableProposals.sol	 PercentD16.sol	 ETHValue.sol
 ImmutableDualGovernanceConfigProvider.sol	 Timestamp.sol	 TimelockedGovernance.sol
 SharesValue.sol	 ResealManager.sol	 IndexOneBased.sol
 Resealer.sol	 ProposalsList.sol	 Executor.sol
 SealableCalls.sol	 ExternalCalls.sol	 DGUpgradeOmnibusMainnet.sol
 DGUpgradeStateVerifierMainnet.sol		

2. Conclusion



Deployment has been successfully validated, meaning that:

- Audited commit matches the deployed contracts fully.
- Default configurations are correct.
- The contracts are ready for use.

Review of fix and service contracts have been successfully completed, meaning that:

- The Escrow.sol fix resolved the issue and did not introduce any new ones.
- The service contracts correctly construct vote data and validate the Dual Governance state following the upgrade.
- No serious vulnerabilities or undisclosed functionality had been found.

Validated commits and audit reports

Repository	Final validated commit	Audit Report	Type
dual-governance	8c77d57a4c415bb69c6873d174be7c30b1103907	2025-02-05	Audit
dual-governance	8c77d57a4c415bb69c6873d174be7c30b1103907	2025-06-05	Deployment

Review

File name	Contract deployed on mainnet
DGUpgradeOmnibusMainnet.sol	0x67988077f29FbA661911d9567E05cc52C51ca1B0
DGUpgradeStateVerifierMainnet.sol	0x487b764a2085ffd595D9141BAec0A766B7904786

Deployment

File name	Contract deployed on mainnet
DualGovernance.sol	0xC1db28B3301331277e307FDCfF8DE28242A4486E
Escrow.sol (Implementation)	0xd6A67636c05BeB5B4a5c90D408b03A63c4e39426
TiebreakerCoreCommittee.sol	0xf65614d73952Be91ce0aE7Dd9cFf25Ba15bEE2f5
TiebreakerSubCommittee.sol (Sub Committee 1)	0x3D3ba54D54bbFF40F2Dfa2A8e27bD4dE3dab2951

TiebreakerSubCommittee.sol (Sub Committee 2)	<u>0xDBfa0B8A15a503f25224fcA5F84a3853230A715C</u>
TiebreakerSubCommittee.sol (Sub Committee 3)	<u>0xBF048f2111497B6Df5E062811f5fC422804D4baE</u>
ImmutableDualGovernanceConfigProvider.sol (for legacy Dual Governance)	<u>0xc934E90E76449F09f2369BB85DCEa056567A327a</u>

STATE MIND