

# STATE MIND

## Dual Governance deployment validation and script review

27-05-2025 - 05-06-2025

# Table of contents



1. Project Brief	2
2. Conclusion	4

# 1. Project Brief



Title	Description
Client	Lido
Project name	Dual Governance deployment validation and script review
Timeline	27-05-2025 - 05-06-2025
Initial commit	7480c3cdc813312c0c36d6faf0f7e6e4148ebfb2, 48b6c8cab4e6498b29e844ca21ae5f3238440771
Final commit	7480c3cdc813312c0c36d6faf0f7e6e4148ebfb2, 48b6c8cab4e6498b29e844ca21ae5f3238440771

## Short Overview

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

The purpose of the validation is to ensure that deployed contracts' sources match the audited commit\* and has the proper parameters. Review of service launch contracts involves verifying their logic and ensuring compliance with the spec regarding permissions transition.

The validation consists of two main parts:

- Dual Governance contracts: dual-governance/contracts
- Sevice launch contracts dual-governance/scripts/launch

Service launch contracts are part of the strategy for transitioning the current governance system to Dual Governance. Given the large number of roles and entities, they streamline the voting process by enumerating the required actions for activation and providing additional checks. The scope includes four contracts:

- DGLaunchOmnibusMainnet.sol: Defines vote items for Aragon Voting to transfer control of key Lido roles and contracts to Dual Governance. Allows validation of a vote in Aragaon against defined items in the contract.
- DGRolesValidatorMainnet.sol: Ensures correct role assignments during both Aragon vote execution and Dual Governance proposal execution. Prevents unauthorized changes and validates proper role transition.
- DGLaunchStateVerifier.sol: Provides verification of the Dual Governance launch state. Confirms successful dry run and checks emergency protection status.
- TimeConstraints.sol: Specifies timing rules for Dual Governance launch phases. Ensures activation and voting meet required timeframes.

## Reference commits and audit reports

Repository	Commit	Audit Report
------------	--------	--------------

dual-governance	3e0f1ae5740ef8410e928f6cc106e3a5f45a5a75*	<u>2025-02-05</u>
-----------------	---	-------------------





































## Notes

\* – The deployment was made from commit 7480c3cdc813312c0c36d6faf0f7e6e4148ebfb2, which differs from the final audited one – 3e0f1ae5740ef8410e928f6cc106e3a5f45a5a75. In the new commit, only comments were modified; the actual code remained unchanged.

As a result, on 7480c3cdc813312c0c36d6faf0f7e6e4148ebfb2 commit the deployed contracts have identical bytecode to those in the audited commit.

## Project Scope

The audit covered the following files:

 <a href="#">Escrow.sol</a>	 <a href="#">AssetsAccounting.sol</a>	 <a href="#">DualGovernance.sol</a>
 <a href="#">EmergencyProtectedTimelock.sol</a>	 <a href="#">HashConsensus.sol</a>	 <a href="#">ExecutableProposals.sol</a>
 <a href="#">DualGovernanceStateMachine.sol</a>	 <a href="#">WithdrawalsBatchesQueue.sol</a>	 <a href="#">Tiebreaker.sol</a>
 <a href="#">EmergencyProtection.sol</a>	 <a href="#">DualGovernanceConfig.sol</a>	 <a href="#">EscrowState.sol</a>
 <a href="#">Proposers.sol</a>	 <a href="#">TiebreakerCoreCommittee.sol</a>	 <a href="#">DualGovernanceStateTransitions.sol</a>
 <a href="#">TiebreakerSubCommittee.sol</a>	 <a href="#">Duration.sol</a>	 <a href="#">TimelockState.sol</a>
 <a href="#">EnumerableProposals.sol</a>	 <a href="#">PercentD16.sol</a>	 <a href="#">ETHValue.sol</a>
 <a href="#">ImmutableDualGovernanceConfigProvider.sol</a>	 <a href="#">Timestamp.sol</a>	 <a href="#">TimelockedGovernance.sol</a>
 <a href="#">SharesValue.sol</a>	 <a href="#">ResealManager.sol</a>	 <a href="#">IndexOneBased.sol</a>
 <a href="#">Resealer.sol</a>	 <a href="#">ProposalsList.sol</a>	 <a href="#">Executor.sol</a>
 <a href="#">SealableCalls.sol</a>	 <a href="#">ExternalCalls.sol</a>	 <a href="#">DGLaunchOmnibusMainnet.sol</a>
 <a href="#">DGRolesValidatorMainnet.sol</a>	 <a href="#">DGLaunchStateVerifier.sol</a>	 <a href="#">TimeConstraints.sol</a>

## 2. Conclusion



Deployment have been successfully validated, meaning that:

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

Review have been successfully completed, meaning that:

- Reviewed commit match the deployed launch service contracts fully.
- The functionality of the launch contracts aligns with the provided specifications\*.
- No serious vulnerabilities or undisclosed functionality had been found.

\* – The DGLaunchOmnibusMainnet.sol contract includes seven additional vote items (51–57). The Lido team has provided comments on each item. The first three items (51–53) are necessary for resetting the RecoveryVaultAppld on DaoKernel, and they also address technical debt related to granting permissions. The remaining items (54–57) include sanity check calls and the Dual Governance proposal.

### Validated commits and audit reports

Repository	Final validated commit	Audit Report
dual-governance	7480c3cdc813312c0c36d6faf0f7e6e4148ebfb2	<u>2025-02-05</u>

### Review

File name	Contract deployed on mainnet
DGLaunchOmnibusMainnet.sol	0x1DB8a9313785b78f7d0a201C5E0BE007f1eb63b4
DGRolesValidatorMainnet.sol	0x31534e3aFE219B609da3715a00a1479D2A2d7981
DGLaunchStateVerifier.sol	0xd48c2fc419569537Bb069BAD2165dC0cEB160CEC
TimeConstraints.sol	0x2a30F5aC03187674553024296bed35Aa49749DDa

### Deployment

File name	Contract deployed on mainnet
EmergencyProtectedTimelock.sol	<u>0xCE0425301C85c5Ea2A0873A2dEe44d78E02D2316</u>

Executor.sol (Admin executor)	<u>0x23E0B465633FF5178808F4A75186E2F2F9537021</u>
DualGovernance.sol	<u>0xcdF49b058D606AD34c5789FD8c3BF8B3E54bA2db</u>
ImmutableDualGovernanceConfigProvider.sol	<u>0xa1692Af6FDfdD1030E4E9c4Bc429986FA64CB5EF</u>
TimelockedGovernance.sol	<u>0x553337946F2FAb8911774b20025fa776B76a7CcE</u>
Escrow.sol (Implementation)	<u>0xb84317C0E142D8911A0d69Dc32c48d87753B8d1C</u>
ResealManager.sol	<u>0x7914b5a1539b97Bd0bbd155757F25FD79A522d24</u>
TiebreakerCoreCommittee.sol	<u>0x175742c3DDD88B0192df3EcF98f180A79cb259D0</u>
TiebreakerSubCommittee.sol (Sub Committee 1)	<u>0x74836470337Ba5d2a92fe16E44AD862E28fcf9B3</u>
TiebreakerSubCommittee.sol (Sub Committee 2)	<u>0xb9d82E1A49f6a66E8a07260BA05Cf9Ac8a938B1C</u>
TiebreakerSubCommittee.sol (Sub Committee 3)	<u>0x7dAdae4e1a0DB43F6bcfA75295666fc044605679</u>

# STATE MIND