

0.7

Lido.fi Process Quality Review

Score: 84%

Overview

This is a Process Quality Review of [Lido.Fi](#) completed on June 7th 2021. It was performed using the Process Review process (version 0.71) and is documented [here](#). The review was performed by Nic of DeFiSafety. Check out our [Telegram](#).

The final score of the review is 84%, a pass. The breakdown of the scoring is in [Scoring Appendix](#). For our purposes, a pass is 70%.

Summary of the Process

Very simply, the review looks for the following declarations from the developer's site. With these declarations, it is reasonable to trust the smart contracts.

- **Here are my smart contracts on the blockchain**
- **Here is the documentation that explains what my smart contracts do**
- **Here are the tests I ran to verify my smart contract**
- **Here are the audit(s) performed on my code by third party experts**
- **Here are the admin controls and strategies**

Disclaimer

This report is for informational purposes only and does not constitute investment advice of any kind, nor does it constitute an offer to provide investment advisory or other services. Nothing in this report shall be considered a solicitation or offer to buy or sell any security, token, future, option or other financial instrument or to offer or provide any investment advice or service to any person in any jurisdiction. Nothing contained in this report constitutes investment advice or offers any opinion with respect to the suitability of any security, and the views expressed in this report should not be taken as advice to buy, sell or hold any security. The information in this report should not be relied upon for the purpose of investing. In preparing the information contained in this report, we have not taken into account the investment needs, objectives and financial circumstances of any particular investor. This information has no regard to the specific investment objectives, financial situation and particular needs of any specific recipient of this information and investments discussed may not be suitable for all investors.

Any views expressed in this report by us were prepared based upon the information available to us at the time such views were written. The views expressed within this report are limited to DeFiSafety and the author and do not reflect those of any additional or third party and are strictly based upon DeFiSafety, its authors, interpretations and evaluation of relevant data. Changed or additional information could cause such

views to change. All information is subject to possible correction. Information may quickly become unreliable for various reasons, including changes in market conditions or economic circumstances.

This completed report is copyright (c) DeFiSafety 2021. Permission is given to copy in whole, retaining this copyright label.

Chain

This section indicates the blockchain used by this protocol.

✓ **Chain: Ethereum**

Guidance:

Ethereum

Binance

Code and Team

This section looks at the code deployed on the Mainnet that gets reviewed and its corresponding software repository. The document explaining these questions is [here](#). This review will answer the questions;

- 1) Are the executing code addresses readily available? (%)
- 2) Is the code actively being used? (%)
- 3) Is there a public software repository? (Y/N)
- 4) Is there a development history visible? (%)
- 5) Is the team public (not anonymous)? (Y/N)

1) Are the executing code addresses readily available? (%)

✓ **Answer: 100%**

They are available at website <https://docs.lido.fi/deployed-contracts> as indicated in the [Appendix](#).

Guidance:

- | | |
|------|--|
| 100% | Clearly labelled and on website, docs or repo, quick to find |
| 70% | Clearly labelled and on website, docs or repo but takes a bit of looking |
| 40% | Addresses in mainnet.json, in discord or sub graph, etc |
| 20% | Address found but labelling not clear or easy to find |
| 0% | Executing addresses could not be found |

How to improve this score

Make the Ethereum addresses of the smart contract utilized by your application available on either your

website or your GitHub (in the README for instance). Ensure the addresses is up to date. This is a very important question wrt to the final score.

2) Is the code actively being used? (%)

✓ Answer: 100%

Activity is 500 transactions a day on contract *deposit_contract.sol*, as indicated in the [Appendix](#).

Percentage Score Guidance

100%	More than 10 transactions a day
70%	More than 10 transactions a week
40%	More than 10 transactions a month
10%	Less than 10 transactions a month
0%	No activity

3) Is there a public software repository? (Y/N)

✓ Answer: Yes

GitHub: <https://github.com/lidofinance>

Is there a public software repository with the code at a minimum, but normally test and scripts also (Y/N). Even if the repo was created just to hold the files and has just 1 transaction, it gets a Yes. For teams with private repos, this answer is No.

4) Is there a development history visible? (%)

✓ Answer: 100%

With 1108 commits and 40 branches, this is a very healthy software repository.

This checks if the software repository demonstrates a strong steady history. This is normally demonstrated by commits, branches and releases in a software repository. A healthy history demonstrates a history of more than a month (at a minimum).


Guidance:

100%	Any one of 100+ commits, 10+branches
70%	Any one of 70+ commits, 7+branches
50%	Any one of 50+ commits, 5+branches
30%	Any one of 30+ commits, 3+branches
0%	Less than 2 branches or less than 10 commits

How to improve this score

Continue to test and perform other verification activities after deployment, including routine maintenance updating to new releases of testing and deployment tools. A public development history indicates clearly to the public the level of continued investment and activity by the developers on the application. This gives a level of security and faith in the application.

5) Is the team public (not anonymous)? (Y/N)

 Answer: No

No public dev identities have been found.

For a yes in this question the real names of some team members must be public on the website or other documentation. If the team is anonymous and then this question is a No.


Documentation

This section looks at the software documentation. The document explaining these questions is [here](#).

Required questions are;

- 6) Is there a whitepaper? (Y/N)
- 7) Are the basic software functions documented? (Y/N)
- 8) Does the software function documentation fully (100%) cover the deployed contracts? (%)
- 9) Are there sufficiently detailed comments for all functions within the deployed contract code (%)
- 10) Is it possible to trace from software documentation to the implementation in code (%)

6) Is there a whitepaper? (Y/N)

 Answer: Yes

Location: <https://docs.lido.fi/>

How to improve this score

Ensure the white paper is available for download from your website or at least the software repository. Ideally update the whitepaper to meet the capabilities of your present application.

7) Are the basic software functions documented? (Y/N)



Answer: Yes

<https://docs.lido.fi/contracts/lido>

How to improve this score

Write the document based on the deployed code. For guidance, refer to the [SecurEth System Description Document](#).

8) Does the software function documentation fully (100%) cover the deployed contracts? (%)



Answer: 80%

<https://docs.lido.fi/contracts/lido> only covers the major functions.

Guidance:

- 100% All contracts and functions documented
- 80% Only the major functions documented
- 79-1% Estimate of the level of software documentation
- 0% No software documentation

How to improve this score

This score can improve by adding content to the requirements document such that it comprehensively covers the requirements. For guidance, refer to the [SecurEth System Description Document](#). Using tools that aid traceability detection will help.

9) Are there sufficiently detailed comments for all functions within the deployed contract code (%)



Answer: 63%

Code examples are in the [Appendix](#). As per the [SLOC](#), there is 63% commenting to code (CtC).

The Comments to Code (CtC) ratio is the primary metric for this score.

Guidance:

- 100% CtC > 100 Useful comments consistently on all code
- 90-70% CtC > 70 Useful comment on most code
- 60-20% CtC > 20 Some useful commenting
- 0% CtC < 20 No useful commenting

How to improve this score

This score can improve by adding comments to the deployed code such that it comprehensively covers the

code. For guidance, refer to the [SecurEth Software Requirements](#).

10) Is it possible to trace from software documentation to the implementation in code (%)

✓ Answer: 100%

There is clear explicit traceability between software documentation and its implementation in code.

Guidance:

- 100% Clear explicit traceability between code and documentation at a requirement level for all code
- 60% Clear association between code and documents via non explicit traceability
- 40% Documentation lists all the functions and describes their functions
- 0% No connection between documentation and code

How to improve this score

This score can improve by adding traceability from requirements to code such that it is clear where each requirement is coded. For reference, check the SecurEth guidelines on [traceability](#).

Testing

This section looks at the software testing available. It is explained in this [document](#). This section answers the following questions;

- 11) Full test suite (Covers all the deployed code) (%)
- 12) Code coverage (Covers all the deployed lines of code, or explains misses) (%)
- 13) Scripts and instructions to run the tests (Y/N)
- 14) Report of the results (%)
- 15) Formal Verification test done (%)
- 16) Stress Testing environment (%)

11) Is there a Full test suite? (%)

✓ Answer: 100%

Code examples are in the [Appendix](#). As per the [SLOC](#), there is 248% testing to code (TtC).

This score is guided by the Test to Code ratio (TtC). Generally a good test to code ratio is over 100%. However the reviewers best judgement is the final deciding factor.

Guidance:

- 100% TtC > 120% Both unit and system test visible

80%	TtC > 80% Both unit and system test visible
40%	TtC < 80% Some tests visible
0%	No tests obvious

How to improve this score

This score can improve by adding tests to fully cover the code. Document what is covered by traceability or test results in the software repository.

12) Code coverage (Covers all the deployed lines of code, or explains misses) (%)

✓ Answer: 85%

Their [Quantstamp audit](#) covers most of the Lido.fi code.

Guidance:

100%	Documented full coverage
99-51%	Value of test coverage from documented results
50%	No indication of code coverage but clearly there is a reasonably complete set of tests
30%	Some tests evident but not complete
0%	No test for coverage seen

How to improve this score

This score can improve by adding tests achieving full code coverage. A clear report and scripts in the software repository will guarantee a high score.

13) Scripts and instructions to run the tests (Y/N)

✓ Answer: Yes

Instructions to run tests can be found at the bottom of <https://github.com/lidofinance/lido-dao>

How to improve this score

Add the scripts to the repository and ensure they work. Ask an outsider to create the environment and run the tests. Improve the scripts and docs based on their feedback.

14) Report of the results (%)

⚠ Answer: 0%


Guidance:

- 100% Detailed test report as described below
- 70% GitHub Code coverage report visible
- 0% No test report evident

How to improve this score


Add a report with the results. The test scripts should generate the report or elements of it.

15) Formal Verification test done (%)

 Answer: 0%

No formal verification of Lido.fi is evident.

16) Stress Testing environment (%)

 Answer: 100%


Multiple test-net smart contract addresses available at <https://docs.lido.fi/deployed-contracts>

Security

This section looks at the 3rd party software audits done. It is explained in this [document](#). This section answers the following questions;

- 17) Did 3rd Party audits take place? (%)
- 18) Is the bounty value acceptably high?

17) Did 3rd Party audits take place? (%)

 Answer: 100%

[Sigma Prime has done a Lido.fi security assessment in December 2020.](#)

[Quantstamp has done a Lido.fi audit in December 2020.](#)


MixBytes has done a Lido.fi audit in [April](#) and [May](#) 2021

Lido.fi was launched December 20th 2021.

Guidance:

- 100% Multiple Audits performed before deployment and results public and implemented or not required
- 90% Single audit performed before deployment and results public and implemented or not required
- 70% Audit(s) performed after deployment and no changes required. Audit report is public
- 50% Audit(s) performed after deployment and changes needed but not implemented
- 20% No audit performed
- 0% Audit Performed after deployment, existence is public, report is not public and no improvements deployed OR smart contract address' not found, question

18) Is the bounty value acceptably high (%)

 Answer: 70%

Bug Bounty program found at <https://immunefi.com/bounty/lido/>.

Guidance:

- 100% Bounty is 10% TVL or at least \$1M AND active program (see below)
- 90% Bounty is 5% TVL or at least 500k AND active program
- 80% Bounty is 5% TVL or at least 500k
- 70% Bounty is 100k or over AND active program
- 50% Bounty is 100k or over
- 40% Bounty is 50k or over
- 20% Bug bounty program bounty is less than 50k
- 0% No bug bounty program offered

Active program means a third party actively driving hackers to the site. Inactive program would be static mention on the docs.

Access Controls

This section covers the documentation of special access controls for a DeFi protocol. The admin access controls are the contracts that allow updating contracts or coefficients in the protocol. Since these contracts can allow the protocol admins to "change the rules", complete disclosure of capabilities is vital for user's transparency. It is explained in this [document](#). The questions this section asks are as follow;

- 19) Can a user clearly and quickly find the status of the admin controls?
- 20) Is the information clear and complete?
- 21) Is the information in non-technical terms that pertain to the investments?
- 22) Is there Pause Control documentation including records of tests?

19) Can a user clearly and quickly find the status of the admin controls (%)

✓ Answer: 100%

Lido.fi uses Aragon as a DAO framework that the base themselves off of. In their docs, they provide operator frameworks at <https://docs.lido.fi/guides/node-operator-manual>

Guidance:

- 100% Clearly labelled and on website, docs or repo, quick to find
- 70% Clearly labelled and on website, docs or repo but takes a bit of looking
- 40% Access control docs in multiple places and not well labelled
- 20% Access control docs in multiple places and not labelled
- 0% Admin Control information could not be found

20) Is the information clear and complete (%)

✓ Answer: 90%

<https://docs.lido.fi/guides/multisig-deployment>

Guidance:

All the contracts are immutable -- 100% OR

- a) All contracts are clearly labelled as upgradeable (or not) -- 30% AND
- b) The type of ownership is clearly indicated (OnlyOwner / MultiSig / Defined Roles) -- 30% AND
- c) The capabilities for change in the contracts are described -- 30%

How to improve this score

Create a document that covers the items described above. An [example](#) is enclosed.

21) Is the information in non-technical terms that pertain to the investments (%)

✓ Answer: 90%

Guidance:

- 100% All the contracts are immutable
- 90% Description relates to investments safety and updates in clear, complete non-software I language
- 30% Description all in software specific language
- 0% No admin control information could not be found

How to improve this score

Create a document that covers the items described above in plain language that investors can understand.

An [example](#) is enclosed.

22) Is there Pause Control documentation including records of tests (%)

✓ Answer: 80%

Pause Control documentation explained at <https://docs.lido.fi/guides/protocol-levers#pausing>, but no evidence of regular tests.

Guidance:

- 100% All the contracts are immutable or no pause control needed and this is explained OR
- 100% Pause control(s) are clearly documented and there is records of at least one test within 3 months
- 80% Pause control(s) explained clearly but no evidence of regular tests
- 40% Pause controls mentioned with no detail on capability or tests
- 0% Pause control not documented or explained

How to improve this score

Create a document that covers the items described above in plain language that investors can understand. An [example](#) is enclosed.

Appendices

Author Details

The author of this review is Rex of DeFi Safety.

Email : rex@defisafety.com Twitter : [@defisafety](https://twitter.com/defisafety)

I started with Ethereum just before the DAO and that was a wonderful education. It showed the importance of code quality. The second Parity hack also showed the importance of good process. Here my aviation background offers some value. Aerospace knows how to make reliable code using quality processes.

I was coaxed to go to EthDenver 2018 and there I started [SecuEth.org](https://secur.eth.org) with Bryant and Roman. We created guidelines on good processes for blockchain code development. We got [EthFoundation funding](#) to assist in their development.

Process Quality Reviews are an extension of the SecurEth guidelines that will further increase the quality processes in Solidity and Vyper development.

DeFiSafety is my full time gig and we are working on funding vehicles for a permanent staff.

Scoring Appendix

PQ Audit Scoring Matrix (v0.7)		Points	Answer	Points
Total		260		217.4
Code and Team				84%
1) Are the executing code addresses readily available? (%)	20	100%	20	
2) Is the code actively being used? (%)	5	100%	5	
3) Is there a public software repository? (Y/N)	5	Y	5	
4) Is there a development history visible? (%)	5	100%	5	
5) Is the team public (not anonymous)? (Y/N)	15	N	0	
Code Documentation				
6) Is there a whitepaper? (Y/N)	5	Y	5	
7) Are the basic software functions documented? (Y/N)	10	Y	10	
8) Does the software function documentation fully (100%) cover the deployed contracts? (%)	15	80%	12	
9) Are there sufficiently detailed comments for all functions within the deployed contract code (%)	5	63%	3.15	
10) Is it possible to trace from software documentation to the implementation in code (%)	10	100%	10	
Testing				
11) Full test suite (Covers all the deployed code) (%)	20	100%	20	
12) Code coverage (Covers all the deployed lines of code, or explains misses) (%)	5	85%	4.25	
13) Scripts and instructions to run the tests? (Y/N)	5	Y	5	
14) Report of the results (%)	10	0%	0	
15) Formal Verification test done (%)	5	0%	0	
16) Stress Testing environment (%)	5	100%	5	
Security				
17) Did 3rd Party audits take place? (%)	70	100%	70	
18) Is the bug bounty acceptable high? (%)	10	70%	7	
Access Controls				
19) Can a user clearly and quickly find the status of the admin controls	5	100%	5	
20) Is the information clear and complete	10	90%	9	
21) Is the information in non-technical terms	10	90%	9	
22) Is there Pause Control documentation including records of tests	10	80%	8	
Section Scoring				
Code and Team		50	70%	
Documentation		45	89%	
Testing		50	69%	
Security		80	96%	
Access Controls		35	89%	

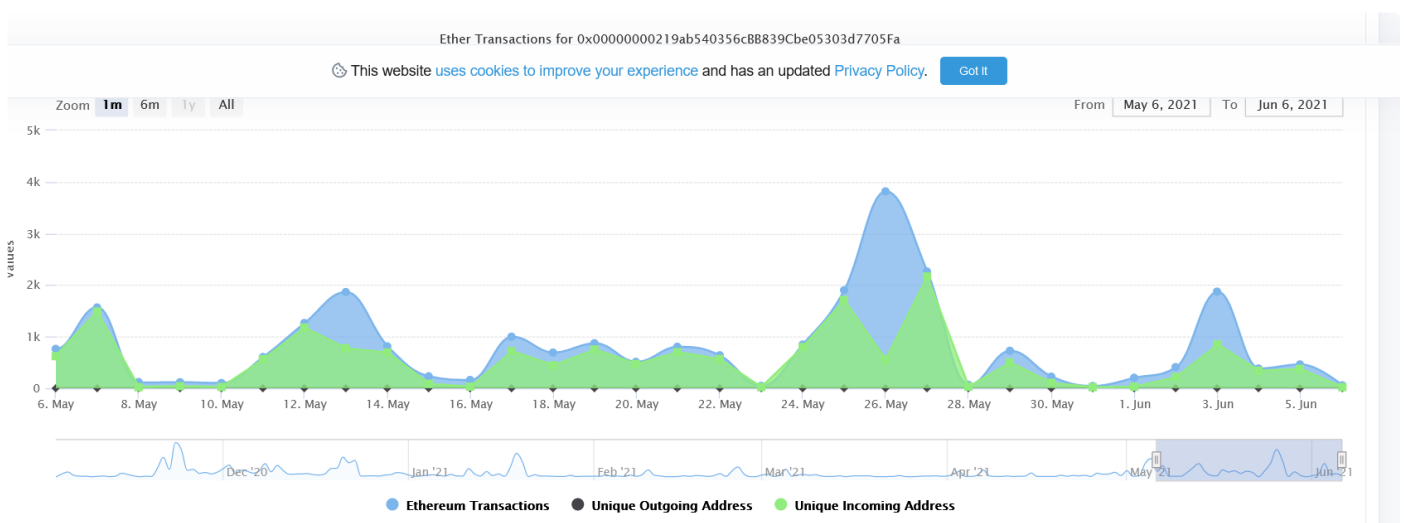
Executing Code Appendix

Core Protocol

- Lido DAO: `0xb8FFC3Cd6e7Cf5a098A1c92F48009765B24088Dc` (proxy)
- LDO token: `0x5A98FcBEA516Cf06857215779Fd812CA3beF1B32`
- Lido and stETH token: `0xae7ab96520DE3A18E5e111B5EaAb095312D7fE84` (proxy)
- wstETH token: `0xae7ab96520DE3A18E5e111B5EaAb095312D7fE84`
- Node Operators registry: `0x55032650b14df07b85bF18A3a3eC8E0Af2e028d5` (proxy)
- Oracle: `0x442af784A788A5bd6F42A01Ebe9F287a871243fb` (proxy)

- Stable Swap Oracle [0x3a6bd15abf19581e411621d669b6a2bbe741ffd6](#)
- stETH Price Feed [0xab55bf4dfbf469ebfe082b7872557d1f87692fe6](#) (proxy)
- Aragon Voting: [0x2e59A20f205bB85a89C53f1936454680651E618e](#) (proxy)
- Aragon Token Manager: [0xf73a1260d222f447210581DDf212D915c09a3249](#) (proxy)
- Aragon Finance: [0xB9E5CBB9CA5b0d659238807E84D0176930753d86](#) (proxy)
- Aragon Agent: [0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c](#) (proxy)

Code Used Appendix



Example Code Appendix

```

1
2 // SPDX-License-Identifier: CC0-1.0
3
4 pragma solidity 0.6.11;
5
6 // This interface is designed to be compatible with the Vyper version.
7 /// @notice This is the Ethereum 2.0 deposit contract interface.
8 /// For more information see the Phase 0 specification under https://github.com/ethereum/e
9 interface IDepositContract {
10     /// @notice A processed deposit event.
11     event DepositEvent(
12         bytes pubkey,
13         bytes withdrawal_credentials,
14         bytes amount,
15         bytes signature,
16         bytes index
17     );
18
19     /// @notice Submit a Phase 0 DepositData object.
20

```

```

    /// @param pubkey A BLS12-381 public key.
21    /// @param withdrawal_credentials Commitment to a public key for withdrawals.
22    /// @param signature A BLS12-381 signature.
23    /// @param deposit_data_root The SHA-256 hash of the SSZ-encoded DepositData object.
24    /// Used as a protection against malformed input.
25    function deposit(
26        bytes calldata pubkey,
27        bytes calldata withdrawal_credentials,
28        bytes calldata signature,
29        bytes32 deposit_data_root
30    ) external payable;
31
32    /// @notice Query the current deposit root hash.
33    /// @return The deposit root hash.
34    function get_deposit_root() external view returns (bytes32);
35
36    /// @notice Query the current deposit count.
37    /// @return The deposit count encoded as a little endian 64-bit number.
38    function get_deposit_count() external view returns (bytes memory);
39 }
40
41 // Based on official specification in https://eips.ethereum.org/EIPS/eip-165
42 interface ERC165 {
43     /// @notice Query if a contract implements an interface
44     /// @param interfaceId The interface identifier, as specified in ERC-165
45     /// @dev Interface identification is specified in ERC-165. This function
46     /// uses less than 30,000 gas.
47     /// @return `true` if the contract implements `interfaceId` and
48     /// `interfaceId` is not 0xffffffff, `false` otherwise
49     function supportsInterface(bytes4 interfaceId) external pure returns (bool);
50 }
51
52 // This is a rewrite of the Vyper Eth2.0 deposit contract in Solidity.
53 // It tries to stay as close as possible to the original source code.
54 /// @notice This is the Ethereum 2.0 deposit contract interface.
55 /// For more information see the Phase 0 specification under https://github.com/ethereum/e
56 contract DepositContract is IDepositContract, ERC165 {
57     uint constant DEPOSIT_CONTRACT_TREE_DEPTH = 32;
58     // NOTE: this also ensures `deposit_count` will fit into 64-bits
59     uint constant MAX_DEPOSIT_COUNT = 2**DEPOSIT_CONTRACT_TREE_DEPTH - 1;
60

```

SLOC Appendix

Solidity Contracts

Language	Files	Lines	Blanks	Comments	Code	Complex
Solidity	34	4181	646	1372	2163	185

Comments to Code 1372/2163 = 63%

Javascript Tests

Language	Files	Lines	Blanks	Comments	Code	Complex
JavaScript	22	7153	1401	393	5359	59

Tests to Code 5359/2163 = 248%