0.7

1inch.exchange Process Quality Review

Score: 85%

Overview

This is a 1inch.exchange Process Quality Review completed on August 9th 2021. It was performed using the Process Review process (version 0.7.3) and is documented here. The review was performed by Nic of DeFiSafety. Check out our Telegram.

The final score of the review is **85%**, a Great **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.

Chain

This section indicates the blockchain used by this protocol.

> **Chain:** Ethereum, Binance Smart Chain, Polygon

Guidance:

Ethereum
Binance Smart Chain
Polygon
Avalanche
Terra

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 following 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://github.com/1inch/liquidity-protocol/blob/master/README.md, 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 labeling not clear or easy to find
0% Executing addresses could not be found

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

> **Answer:** 100%

Activity is over 10 transactions a day on contract *MooniswapFactory.sol*, as indicated in the Appendix.

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/1inch/liquidity-protocol.

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

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

> **Answer:** 100%

With 578 commits and 7 branches, this is a very healthy repository.

This metric 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 30 commits

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

> **Answer:** Yes

Location: https://blog.1inch.io/meet-1inch-team-anton-bukov-co-founder-and-cto-9d0d1b56142b.

For a **"Yes"** in this question, the real names of some team members must be public on the website or other documentation (LinkedIn, etc). If the team is anonymous, 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.1inch.io/api/.

Note: Previous whitepaper was deprecated, and a link to this API doc was provided instead.

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

> **Answer:** Yes

There are basic software functions documented in the 1inch API documentation.

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

> ✓ **Answer:** 80%

Most of the core software functions are documented in the API documentation, as well as in the READ.me of their liquidity-protocol repository.

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 be improved by adding content to the software functions 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:** 0%

Code examples are in the Appendix. As per the SLOC, there is 4% commenting to code (CtC).

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

Note: Interface, library, mock, and utility files were not used in this calculation. Only the core solidity contract files were used.

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 and explicit traceability when it comes to the 1inch software documentation and its implementation within their source code, as seen in the "Quote/Swap" section, this READ.me, and the swagger documentation.

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

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 171% 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

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

> **Answer:** 77%

There is 77% code coverage according to this codecov report.

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 improved by adding tests that achieve 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**

Scrips/Instructions location: The 1inch API docs serve as instructions to run whichever tests you want.

14) Report of the results (%)

> **Answer:** 70%

The GitHub code coverage report is visible.

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 evidence of a 1inch Formal Verification test was found in their documentation or in further web searches.

16) Stress Testing environment (%)

> **Answer:** 100%

There is evidence of Kovan testnet smart contract usage in the "Deployment" repository of the 1inch GitHub.

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%

There have been multiple audits performed on the 1inch contracts before and after their various deployments (v1-v3). The full list of audits can be found here.

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, (where question 1 is 0%)

Deduct 25% if code is in a private repo and no note from auditors that audit is applicable to deployed code

18) Is the bounty value acceptably high (%)

> **Answer:** 0%

There is evidence of a 1inch bug bounty program, but no details regarding the potential rewards offered to participating users.

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
60% Bounty is 100k or over
50% Bounty is 50k or over AND active program
40% Bounty is 50k or over
20% Bug bounty program bounty is less than 50k
0% No bug bounty program offered

An active program means that a third party (such as Immunefi) is actively driving hackers to the site. An inactive program would be static mentions 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 access controls (%)

> **Answer:** 100%

1inch admin access control information can easily be found at the bottom of the governance section of their website at https://gov.1inch.io/.

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: 10**0%

All of the relevant information is described here. The contracts are immutable.

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%

All descriptions of the 1inch governance model are user-friendly, complemented with graphs and imagery, as well as adequately detailing each aspect of the governance model at https://blog.1inch.io/1inch-token-is-released-e69ad69cf3ee. However they never actually say their contracts cannot be upgraded.

The commenting in the executing governance contracts is also helpful.

Guidance:

100%	All the contracts are immutable
90%	Description relates to investments safety and updates in clear, complete non-software l 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:** 0%

No Pause Guardian or similar function was found in the 1inch documentation. However the contracts have pause capability.

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

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 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.

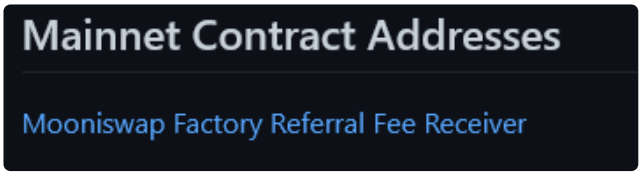
DeFiSafety is my full time gig and we are working on funding vehicles for a permanent staff.

Scoring Appendix

	Total	1inch v.07 UPDATE	
PQ Audit Scoring Matrix (v0.7)	**Points**	**Answer**	**Points**
Total	**260**		220.85
Code and Team			**85%**
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**	Y	15

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**	0%	0
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**	77%	3.85
13) Scripts and instructions to run the tests? (Y/N)	**5**	Y	5
14) Report of the results (%)	**10**	70%	7
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**	0%	0
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**	0%	0
Section Scoring			
Code and Team	50	100%	
Documentation	45	82%	
Testing	50	82%	
Security	80	88%	
Access Controls	35	66%	

Executing Code Appendix



Code Used Appendix

0xd0e4dc9c48d65d40de...	12992804	3 mins ago	0xa0446d8804611944f1...	→	0xbaf9a5d4b005235932...	0 Ether
0x86a562fb7790939d6f...	12992801	3 mins ago	0x0e1953f27e64ea9dad...	→	0xbaf9a5d4b005235932...	0 Ether
0x86a562fb7790939d6f...	12992801	3 mins ago	0x0e1953f27e64ea9dad...	→	0xbaf9a5d4b005235932...	0 Ether
0x86a562fb7790939d6f...	12992801	3 mins ago	0x0e1953f27e64ea9dad...	→	0xbaf9a5d4b005235932...	0 Ether
0x6ac3167e9ecb070656...	12992779	8 mins ago	0xe991f8901ea1cc31e4...	→	0xbaf9a5d4b005235932...	0 Ether
0x6ac3167e9ecb070656...	12992779	8 mins ago	0xe991f8901ea1cc31e4...	→	0xbaf9a5d4b005235932...	0 Ether
0x6ac3167e9ecb070656...	12992779	8 mins ago	0xe991f8901ea1cc31e4...	→	0xbaf9a5d4b005235932...	0 Ether
0x3f453958385db563b7...	12992772	9 mins ago	0xa0446d8804611944f1...	→	0xbaf9a5d4b005235932...	0 Ether
0x41b6b232be1395e6e...	12992719	20 mins ago	0x9696d4999a2576671...	→	0xbaf9a5d4b005235932...	0 Ether
0x41b6b232be1395e6e...	12992719	20 mins ago	0x9696d4999a2576671...	→	0xbaf9a5d4b005235932...	0 Ether
0x43d90adaf6269031e1...	12992671	30 mins ago	0xad8c42021ba682c69a...	→	0xbaf9a5d4b005235932...	0 Ether
0x43d90adaf6269031e1...	12992671	30 mins ago	0xad8c42021ba682c69a...	→	0xbaf9a5d4b005235932...	0 Ether
0x317e82e02663a0744...	12992656	33 mins ago	0x80b9cb40f05785f03ae...	→	0xbaf9a5d4b005235932...	0 Ether
0x317e82e02663a0744...	12992656	33 mins ago	0x80b9cb40f05785f03ae...	→	0xbaf9a5d4b005235932...	0 Ether
0xaae11d85468dd3d42c...	12992643	36 mins ago	0x0f0e6e11dccb4d08cd...	→	0xbaf9a5d4b005235932...	0 Ether
0xaae11d85468dd3d42c...	12992643	36 mins ago	0x0f0e6e11dccb4d08cd...	→	0xbaf9a5d4b005235932...	0 Ether

0xc516392284cc46123b...	12992637	38 mins ago	0x0f0e6e11dccb4d08cd...	→	0xbaf9a5d4b005235932...	0 Ether
0xc516392284cc46123b...	12992637	38 mins ago	0x0f0e6e11dccb4d08cd...	→	0xbaf9a5d4b005235932...	0 Ether
0x728fa5a3e88cfb61164...	12992622	42 mins ago	0xad8c42021ba682c69a...	→	0xbaf9a5d4b005235932...	0 Ether
0x728fa5a3e88cfb61164...	12992622	42 mins ago	0xad8c42021ba682c69a...	→	0xbaf9a5d4b005235932...	0 Ether
0x5a32907fb9102dd9e1...	12992613	44 mins ago	0x1dce26f543e591c277...	→	0xbaf9a5d4b005235932...	0 Ether
0x5a32907fb9102dd9e1...	12992613	44 mins ago	0x1dce26f543e591c277...	→	0xbaf9a5d4b005235932...	0 Ether
0x5a32907fb9102dd9e1...	12992613	44 mins ago	0x1dce26f543e591c277...	→	0xbaf9a5d4b005235932...	0 Ether

Example Code Appendix

```
contract MooniswapFactory is IMooniswapFactory, MooniswapFactoryGovernance {
    using UniERC20 for IERC20;

    event Deployed(
        Mooniswap indexed mooniswap,
        IERC20 indexed token1,
        IERC20 indexed token2
    );

    IMooniswapDeployer public immutable mooniswapDeployer;
    address public immutable poolOwner;
    Mooniswap[] public allPools;
    mapping(Mooniswap => bool) public override isPool;
    mapping(IERC20 => mapping(IERC20 => Mooniswap)) private _pools;

    constructor (address _poolOwner, IMooniswapDeployer _mooniswapDeployer, address _governance)
        poolOwner = _poolOwner;
        mooniswapDeployer = _mooniswapDeployer;
    }

    function getAllPools() external view returns(Mooniswap[] memory) {
        return allPools;
    }

    function pools(IERC20 tokenA, IERC20 tokenB) external view override returns (Mooniswap
        (IERC20 token1, IERC20 token2) = sortTokens(tokenA, tokenB);
        return _pools[token1][token2];
    }

    function deploy(IERC20 tokenA, IERC20 tokenB) public returns(Mooniswap pool) {
        require(tokenA != tokenB, "Factory: not support same tokens");
        (IERC20 token1, IERC20 token2) = sortTokens(tokenA, tokenB);
        require(_pools[token1][token2] == Mooniswap(0), "Factory: pool already exists");

        string memory symbol1 = token1.uniSymbol();
        string memory symbol2 = token2.uniSymbol();

        pool = mooniswapDeployer.deploy(
            token1,
            token2,
```

```
            string(abi.encodePacked("1inch Liquidity Pool (", symbol1, "-", symbol2, ")")),
            string(abi.encodePacked("1LP-", symbol1, "-", symbol2)),
            poolOwner
        );

        _pools[token1][token2] = pool;
        allPools.push(pool);
        isPool[pool] = true;

        emit Deployed(pool, token1, token2);
    }

    function sortTokens(IERC20 tokenA, IERC20 tokenB) public pure returns(IERC20, IERC20) {
        if (tokenA < tokenB) {
            return (tokenA, tokenB);
        }
        return (tokenB, tokenA);
    }
}
```

SLOC Appendix

Solidity Contracts

Language	Files	Lines	Blanks	Comments	Code	Complex
Solidity	9	1349	263	37	1049	137

Comments to Code 37/1049 = 4%

Javascript Tests

Language	Files	Lines	Blanks	Comments	Code	Complex
JavaScript	7	2248	373	79	1796	43

Tests to Code 1796/1049 = 171%