# 0.7

## Nexus Mutual 0.7 Update Process Quality Review

Score: 80%

## Overview

This is a Nexus Mutual Process Quality Review completed on 15/09/2021. It was performed using the Process Review process (version 0.7.3) and is documented here. The review was performed by Nick of DeFiSafety. Check out our Telegram.

The final score of the review is **80%**, 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.



**Chain**

This section indicates the blockchain used by this protocol.

> **Chain:** Ethereum

**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://api.nexusmutual.io/version-data/, 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, when combining internal and external transactions, on contract 0x84EdfFA16bb0b9Ab1163abb0a13Ff0744c11272f 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/NexusMutual

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%

An impressive 2,248 commits with 10 branches details a rich development history.

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://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf

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://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf

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

> **Answer:** Yes

This protocol has clear function documentation.

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

> **Answer:** 50%

The documentation covers all deployed contracts, but there is little explanation.

**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 |

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

**Answer:** 27%

Code examples are in the Appendix. As per the SLOC, there is 27% 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:** 0%

A deployment contract has not been clearly explained with explicit traceability, and other traceability is nonexplicit between the documents and the protocol's GitHub.

**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 documentation to code such that it is clear where each outlined function is coded in the source code. 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:** 80%

Code examples are in the Appendix. As per the SLOC, there is 87% 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:** 69%

The code coverage is documented here.

**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:** https://github.com/NexusMutual/smart-contracts

**14) Report of the results (%)**

> ⚠ **Answer: 0%**

There is no test report.

**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 was found.

**16) Stress Testing environment (%)**

> ✓ **Answer:** 100%

The documents mention projects undergoing testing in addition to documented Kovan testing.

---

## 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%

Three audits have taken place in which the results have been published. The most recent was in May, 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, (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:** 50%

Nexus Mutual operates an active bounty program with a maximum reward of $50,000.

**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%

The access controls are easily located in the documents.

**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%

a) All contracts are clearly labelled as upgradeable (or not) -- 30% -- the contracts & how governance can change them are clearly explained.