Process Quality Review (0.9)

Ensuro

Final score %

Date: 18 Mar 2024

Audit Process: version 0.9

Author: Rex

PQR Score: 93% PASS

Protocol Website: https://ensuro.co/

Scoring Appendix

The final review score is indicated as a percentage. The percentage is calculated as Achieved Points due to MAX Possible Points. For each element the answer can be either Yes/No or a percentage. For a detailed breakdown of the individual weights of each question, please consult this document.

The blockchain used by this protocol

Polygon

#	Question	Answer
	Code and Team	**100%**
1.	Are the smart contract addresses easy to find? (%)	100%
2.	Does the protocol have a public software repository? (Y/N)	Yes
3.	Is the team public (not anonymous)?	100%
4.	How responsive are the devs when we present our initial report?	100%
	Code Documentation	**92%**
5.	Is there a whitepaper? (Y/N)	Yes
6.	Is the protocol's software architecture documented? (%)	100%
7.	Does the software documentation fully cover the deployed contracts' source code? (%)	100%
8.	Is it possible to trace the documented software to its implementation in the protocol's source code? (%)	60%
9.	Is the documentation organized to ensure information availability and clarity? (%)	100%
	Testing	**91%**
10.	Has the protocol tested their deployed code? (%)	100%
11.	How covered is the protocol's code? (%)	98%
12.	Is there a detailed report of the protocol's test results?(%)	100%
13.	Has the protocol undergone Formal Verification? (Y/N)	No
	Security	**94%**
14.	Is the protocol sufficiently audited? (%)	100%
15.	Is there a matrix of audit applicability on deployed code (%)? Please refer to the example doc for reference.	100%
16.	Is the bug bounty value acceptably high (%)	60%
17.	Is there documented protocol monitoring (%)?	80%
18.	Is there documented protocol front-end monitoring (%)?	100%

Admin Controls		91%
19.	Is the protocol code immutable or upgradeable? (%)	80%
20.	Is the protocol's code upgradeability clearly explained in non technical terms? (%)	100%
21.	Are the admin addresses, roles and capabilities clearly explained? (%)	100%
22.	Are the signers of the admin addresses clearly listed and provably distinct humans? (%)	100%
23.	Is there a robust documented transaction signing policy? Please refer to the Example doc for reference.(%)	90%
	Total:	**93%**

Summary

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 contract on the blockchain(s)
- Here is the documentation that explains what my smart contracts do
- Here are the tests I ran to verify my smart contracts
- Here are all the security steps I took to safeguard these contracts
- Here is an explanation of the control I have to change these smart contracts
- Here is how these smart contracts get information from outside the blockchain (if applicable)

Disclaimer

Code and Team 100%

This section looks at the code deployed on the relevant chains and team aspects. The document explaining these questions is here.

1. Are the smart contract addresses easy to find? (%)

Answer: **100%**

Smart Contract addresses are in the GitBook.

Percentage Score Guidance:

100%	Clearly labelled and on website, documents or repository, 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. Does the protocol have a public software repository? (Y/N)

Answer: Yes

Yes, but it is quite difficult to find. On the Architecture page of the documents you have to click on "open source". There is no link indicating the GitHub address clearly.

Score Guidance:

Yes	There is 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.
No	For teams with private repositories.

3. Is the team public (not anonymous)?

Answer: **100%**

The team is public and listed on they about page of their website.

Percentage Score Guidance:

100%	At least two names can be easily found in the protocol's website, documentation or medium. These are then confirmed by the personal websites of the individuals / their linkedin / twitter.
50%	At least one public name can be found to be working on the protocol.
0%	No public team members could be found.

4. How responsive are the devs when we present our initial report?

Answer: **100%**

Devs answered real quick.

Percentage Score Guidance:

100%	Devs responded within 24hours
75%	Devs responded within 48 hours
50%	Devs responded within 72 hours
25%	Data not entered yet
0%	no dev response within 72 hours

Code Documentation 92%

This section looks at the software documentation. The document explaining these questions is here.

5. Is there a whitepaper? (Y/N)

Answer: Yes

White paper link can be found on the architecture page.

Score Guidance:

Yes	There is an actual whitepaper or at least a very detailed doc on the technical basis of the protocol.
No	No whitepaper. Simple gitbook description of the protocol is not sufficient.

6. Is the protocol's software architecture documented? (%)

Answer: **100%**

There is comprehensive architecture description on the Architecture page and the subsequent pages on each smart contract aspects as found here.

Percentage Score Guidance:

100%	Detailed software architecture diagram with explanation
75%	Basic block diagram of software aspects
0%	No software architecture documentation

7. Does the software documentation fully cover the deployed contracts' source code? (%)

Answer: **100%**

There is strong software documentation starting from the Contracts page and moving down through each smart contract. This drives a score of 100%.

Percentage Score 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

8. Is it possible to trace the documented software to its implementation in the protocol's source code? (%)

Answer: **60%**

60% Clear association between code and documents via non explicit traceability

Percentage Score Guidance:

100%	will be Requirements with traceability to code and to tests (as in avionics DO-178)
90%	on formal requirements with some traceability
80%	for good autogen docs https://developers.morpho.xyz/
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

9. Is the documentation organized to ensure information availability and clarity? (%)

Answer: **100%**

The documentation is clearly organized and easy to navigate.

Percentage Score Guidance:

100%	Information is well organized, compartmentalized and easy to navigate
50%	information is decently organized but could use some streamlining
0%	information is generally obfuscated

Testing 91%

This section covers the testing process of the protocol's smart contract code previous to its deployment on the mainnet. The document explaining these questions is here.

10. Has the protocol tested their deployed code? (%)

Answer: **100%**

Test to Code = 10601 / 5267 = 196% which gives a score of 100% as per guidance.

Percentage Score 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

11. How covered is the protocol's code? (%)

Answer: **98%**

Code coverage is indicated as 97.7%. This is listed at the top of the readme.

Percentage Score 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 complete set of tests
30%	Some tests evident but not complete
0%	No test for coverage seen

12. Is there a detailed report of the protocol's test results?(%)

Answer: **100%**

All test data is available from the GitHub links. This gives a 100% score.

Percentage Score Guidance:

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

13. Has the protocol undergone Formal Verification? (Y/N)

Answer: No

No formal verification tests are apparent.

Score Guidance:

Yes	Formal Verification was performed and the report is readily available
No	Formal Verification was not performed and/or the report is not readily available.

Security 94%

This section looks at the 3rd party software audits done. It is explained in this document.

14. Is the protocol sufficiently audited? (%)

Answer: **100%**

There are two audits from a very reputable auditors. The indicate problems found were resolved before deployment. This drives a score of 100%,

Percentage Score Guidance:

100%	Multiple Audits performed before deployment and the audit findings are public and implemented or not required
90%	Single audit performed before deployment and audit findings are public and implemented or not required
70%	Audit(s) performed after deployment and no changes required. The Audit report is public.
65%	Code is forked from an already audited protocol and a changelog is provided explaining why forked code was used and what changes were made. This changelog must justify why the changes made do not affect the audit.
50%	Audit(s) performed after deployment and changes are needed but not implemented.
30%	Audit(s) performed are low-quality and do not indicate proper due diligence.
20%	No audit performed
0%	Audit Performed after deployment, existence is public, report is not public OR smart contract address' not found.

Deduct 25% if the audited code is not available for comparison.

15. Is there a matrix of audit applicability on deployed code (%)? Please refer to the example doc for reference.

Answer: **100%**

The list of audits very clearly indicates the applicability of the audits and what is not yet audited.

Percentage Score Guidance:

100%	Current and clear matrix of applicability
50%	Out of date matrix of applicability
0%	no matrix of applicability

16. Is the bug bounty value acceptably high (%)

Answer: **60%**

There is a bug bounty with Immunifi. The maximum bounty is only $30,000. This drives a score of 20%. Except the TVL of ensuro is 580k, making the 30k bounty equal to 5% of TVL (for now). As the amount is capped and not connected to the TVL, we will give a 60% score, rather than 80%.

Percentage Score 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 / the bug bounty program is dead

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.

17. Is there documented protocol monitoring (%)?

Answer: **80%**

40% for documentation covering operational monitoring In the real-time monitoring section. On the Governance Page they mentioned using Forta bots and OpenZep Defencder to dynamically measures security risk. This is in the Restricted Executor section. This as another 40% for a total of 80%.

Percentage Score Guidance:

100%	Multiple Audits performed before deployment and results public and implemented or not required
80%	Documentation covering protocol specific threat monitoring
60%	Documentation covering generic threat with incident response
40%	Documentation covering operational monitoring with incident response
0%	No on chain monitoring

Add 20% for documented incident response process

18. Is there documented protocol front-end monitoring (%)?

Answer: **100%**

There is a full-page describing the security infrastructure for the webpage development. This drives a score of 100%.

Percentage Score Guidance:

25%	DDOS Protection
25%	DNS steps to protect the domain
25%	Intrusion detection protection on the front end
25%	Unwanted front-end modification detection

Admin Controls 91%

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.

19. Is the protocol code immutable or upgradeable? (%)

Answer: **80%**

Contracts are upgradeable with roles and timelock. Score 80%.

Percentage Score Guidance:

100%	Fully Immutable
80%	Updateable with Timelock > 1wk
50%	Updateable code with Roles
30%	Updateable code MultiSig
0%	Updateable code via EOA

Pause control does not impact immutability

20. Is the protocol's code upgradeability clearly explained in non technical terms? (%)

Answer: **100%**

The upgradability is clearly explained in the Governance section

Percentage Score Guidance:

100%	Code is Immutable and clearly indicated so in documentation OR
100%	Code is upgradeable and clearly explained in non technical terms
50%	Code is upgradeable with minimal explanation
50%	Code is immutable but this is not mentioned clearly in the documentation
0%	No documentation on code upgradeability

21. Are the admin addresses, roles and capabilities clearly explained? (%)

Answer: **100%**

The roles and capability are clearly listed in the Governance page.

Percentage Score Guidance:

100%	Admin addresses, roles and capabilities clearly explained OR
100%	If immutable code and no changes possible, no admins required
80%	Admin addresses, roles and capabilities incompletely explained but good content
40%	Admin addresses, roles and capabilities minimally explained, information scattered
0%	No information on admin addresses, roles and capabilities

22. Are the signers of the admin addresses clearly listed and provably distinct humans? (%)

Answer: **100%**

The signers and addresses of the MultiSync's are clearly listed on the Governance page. As their names and LinkedIn profiles are listed, they are counted as provably distinct humans. This gives a score of 100%.

Percentage Score Guidance:

100%	All signers of the admin addresses are clearly listed and provably distinct humans OR
100%	If immutable code and no changes possible, therefore no admins
60%	All signers of the admin addresses are clearly listed
30%	Some signers of the admin addresses are listed
0%	No documentation on the admin addresses

23. Is there a robust documented transaction signing policy? Please refer to the Example doc for reference.(%)

Answer: **90%**

There is a Transaction Signing policy section in the Governments page. It indicates a number of good transaction requirements (MultiSig, isolated environment, hardware wallet) and and auditing process through the Bermuda Monetary Authority. All of This Drives a Score of 90%.

Percentage Score Guidance:

100%	If immutable and no changes possible
80%	Robust transaction signing process (7 or more elements)
70%	Adequate transaction signing process (5 or more elements)
60%	Weak transaction signing process (3 or more elements)
0%	No transaction signing process evident

Evidence of audits of signers following the process add 20%