Process Quality Review (0.9)

Biconomy Nexus

Final score %
92
DEFISAFETY

Date: 21 Oct 2024

Audit Process: version 0.9

Author: Rex

PQR Score: 92% PASS

Protocol Website: https://www.biconomy.io/post/nexus-modular-smart-account

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

Ethereum

#	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	**88%**
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? (%)	40%
9.	Is the documentation organized to ensure information availability and clarity? (%)	100%
	Testing	**85%**
10.	Has the protocol tested their deployed code? (%)	100%
11.	How covered is the protocol's code? (%)	100%
12.	Is there a detailed report of the protocol's test results?(%)	70%
13.	Has the protocol undergone Formal Verification? (Y/N)	No
	Security	**88%**
14.	Is the protocol sufficiently audited? (%)	90%
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 (%)?	100%
18.	Is there documented protocol front-end monitoring (%)?	100%

	Admin Controls	100%
19.	Is the protocol code immutable or upgradeable? (%)	100%
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.(%)	100%
	Total:	92%

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

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 2023. Permission is given to copy in whole, retaining this copyright label.

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%**

Not Applicable.

The Biconomy Nexus is a suite of software that can be plugged into a smart contract enabling account obstruction functionality. This means it is not deployed and therefore does not have an address in the same way that a DeFi protocol would. We will give 100%, but actually it is not applicable.

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 labelling 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

Location: https://github.com/bcnmy/nexus

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%**

Yes, The team is clearly listed.

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%**

The team was very responsive and enthusiastic about the review.

Percentage Score Guidance:

100%	Devs responded within 24hours
100%	Devs slow but very active in improving the report
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 88%

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

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

Answer: **Yes**

Location: https://github.com/bcnmy/nexus/wiki

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%**

Yes, there is a detailed smart contract architecture page with diagrams and text giving all required information.

Percentage Score Guidance:

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

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

Answer: **100%**

With the combination of the contract descriptions in the "Core Components" section of the Network Architecture page plus the excellent documentation in the code itself brings an overall 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: **40%**

Documentation is very thorough but there is no traceability. This leads to a score of 40%.

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
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%**

Documentation organization is excellent throughout.

Percentage Score Guidance:

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

Testing 85%

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 = 17317/4124 = 419% 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: **100%**

Coverage is 100% as indicated in the GitHub (Foundry coverage).

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: **70%**

Coverage Report is in the GitHub

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 appears evident.

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 88%

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

14. Is the protocol sufficiently audited? (%)

Answer: **90%**

There is an excellent code competition results from CodeHawks. Report is public and results have been implemented. Plus a second Spearbit audit. Score 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%**

Not required as there is just a single audit

Percentage Score Guidance:

100%	Current and clear matrix of applicability
100%	4 or less clearly relevant audits
50%	Out of date matrix of applicability
0%	no matrix of applicability

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

Answer: **60%**

The bug bounty program is clearly described in the security document. The rewards for a critical bug on 50 K. The bug bounty program is self managed. As Biconomy is not a protocol and as such does not have the assets a DeFi protocol would have we will give a score of 60% rather than the 40% that 50 K unmanaged would normally offer.

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: **100%**

Not applicable as this is not a deployed software

Percentage Score Guidance:

80%	Documentation covering protocol specific threat monitoring
60%	Documentation covering generic threat monitoring
40%	Documentation covering operational monitoring
0%	No on chain monitoring

Add 20% for documented incident response process

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

Answer: **100%**

Not applicable as this is not deployed software.

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 OR
60%	For a generic web site protection statement

Admin Controls 100%

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: **100%**

Not applicable as this is not deployed software.

Percentage Score Guidance:

100%	Fully Immutable
90%	Updateable via Governance with a timelock >= 5 days
80%	Updateable with Timelock >= 5 days
70%	Updateable via Governance
50%	Updateable code with Roles
40%	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%**

Not applicable as this is not deployed software.

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%**

Not applicable as this is not deployed software.

Percentage Score Guidance:

100%	If immutable code and no changes possible, no admins required OR
100%	Admin addresses, roles and capabilities clearly explained OR
100%	Admin control is through Governance and process clearly explained
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%**

Not applicable as this is not deployed software.

Percentage Score Guidance:

100%	If immutable and no changes possible
100%	If admin control is fully via governance
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%

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

Answer: **100%**

Not applicable as this is not deployed software.

Percentage Score Guidance:

100%	If immutable and no changes possible
100%	If admin control is fully via governance
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%