PQ Review Process Differences

Description of changes for Process Evolution

Versions

0.7.3 July 2021

Added : **Each contract address must have the software visible in Etherscan. Bytecode only for the contract is equivalent to no address.** in the Q1 section. This is because of Wing Finance that published their addresses but the contracts were hidden and no GitHub.

0.7.2 June 2021

Changed Guidance on Q18 Bug Bounty to

60%	Bounty is 100k or over
50%	Bounty is 50k or over AND active program
40%	Bounty is 50k or over

from:

50%	Bounty is 100k or over
40%	Bounty is 50k or over

0.71 June 2021

Added to Guidance on Audits:
50% Audit(s) performed after deployment and changes are needed but not implemented

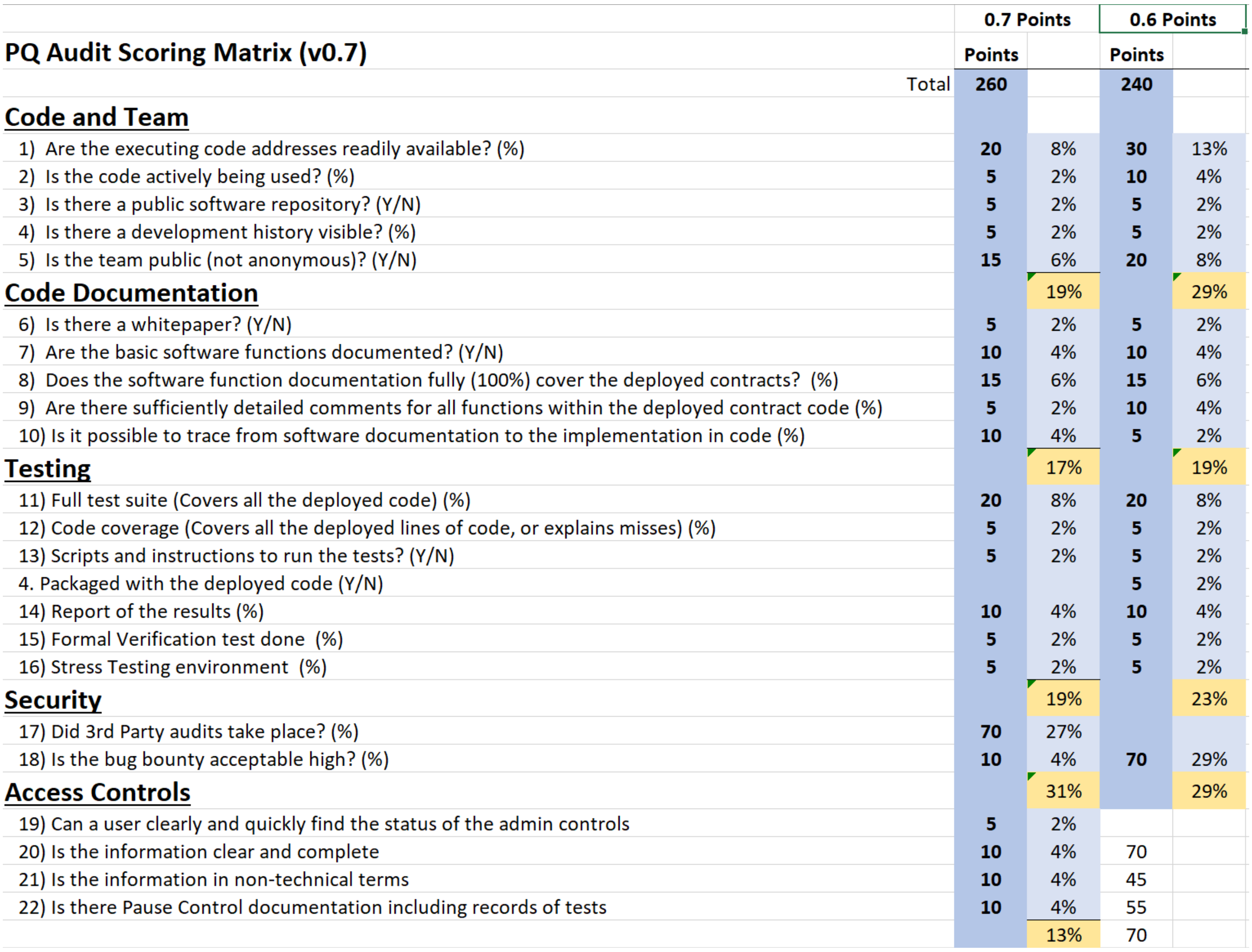
0.7 May 2021

Big Changes

1) Added Access Controls section
2) Added multi chain review capability
3) Added bug bounty question

All Changes

1) Added Access Controls section
2) Added multi chain review capability
3) Removed the question "Packaged with the deployed code (Y/N)" from testing as it added little value (always YES)
4) Added numbers to the questions, to make reference easier
5) Added Overview title at the start of the review
6) Changed the section name from "Audits" to "Security" as it now has Audits and Bug Bounty questions
7) Weight Changes (see below)



	0.7 Points		0.6 Points	
PQ Audit Scoring Matrix (v0.7)	**Points**		**Points**	
Total	**260**		**240**	
Code and Team				
1) Are the executing code addresses readily available? (%)	**20**	8%	**30**	13%
2) Is the code actively being used? (%)	**5**	2%	**10**	4%
3) Is there a public software repository? (Y/N)	**5**	2%	**5**	2%
4) Is there a development history visible? (%)	**5**	2%	**5**	2%
5) Is the team public (not anonymous)? (Y/N)	**15**	6%	**20**	8%
Code Documentation		19%		29%
6) Is there a whitepaper? (Y/N)	**5**	2%	**5**	2%
7) Are the basic software functions documented? (Y/N)	**10**	4%	**10**	4%
8) Does the software function documentation fully (100%) cover the deployed contracts? (%)	**15**	6%	**15**	6%
9) Are there sufficiently detailed comments for all functions within the deployed contract code (%)	**5**	2%	**10**	4%
10) Is it possible to trace from software documentation to the implementation in code (%)	**10**	4%	**5**	2%
Testing		17%		19%
11) Full test suite (Covers all the deployed code) (%)	**20**	8%	**20**	8%
12) Code coverage (Covers all the deployed lines of code, or explains misses) (%)	**5**	2%	**5**	2%
13) Scripts and instructions to run the tests? (Y/N)	**5**	2%	**5**	2%
4. Packaged with the deployed code (Y/N)			**5**	2%
14) Report of the results (%)	**10**	4%	**10**	4%
15) Formal Verification test done (%)	**5**	2%	**5**	2%
16) Stress Testing environment (%)	**5**	2%	**5**	2%
Security		19%		23%
17) Did 3rd Party audits take place? (%)	**70**	27%		
18) Is the bug bounty acceptable high? (%)	**10**	4%	**70**	29%
Access Controls		31%		29%
19) Can a user clearly and quickly find the status of the admin controls	**5**	2%		
20) Is the information clear and complete	**10**	4%	70	
21) Is the information in non-technical terms	**10**	4%	45	
22) Is there Pause Control documentation including records of tests	**10**	4%	55	
		13%	70	

0.6.2 February 2021

Added "For our purposes, a pass is 70%." after Scoring section at the start.

0.6.1 December 2020

Added % guidance for Report of the Results in the Testing section

0.6 -- 6 November 2020

Overview

1. Improved “Summary of the Process”
2. Improved Disclaimer after legal review
3. Improved “Sections of the Review Process” to match the revised report
4. Changed the Scoring rubric to match all 0.6 changes
5. Added “Private Software Repos” section

Code and Team

1. Improve the wording in the “Are the executing code addresses readily available? (Y/N)” question to emphasize its importance and the impact of not having the addresses public.
2. Removed the question; "Are the Contracts Verified?". This question asks if the contracts are "verified" on Etherscan. Frankly, it was always true on every review we did. For this reason, I am removing the question as it adds no value.
3. Changed the question " Does the code match a tagged version on a code hosting platform" to "Is There a Public Software Repository". Finding and matching all the contracts was time-consuming and added little value.
4. Change the question from "Is the Software Repository Healthy" to "Is There Development History Visible?". This is effectively the same question asked in a different way. When asked this way the software repository is not mandatory, merely convenient.
5. Added the question “Is the team public (not anonymous)? (Y/N)” as this is an element of trust we felt needed to be added.

Documentation

1. Improved the wording in the "Is there a white paper?" question allowing medium articles also
2. Change the wording of the question from "Do the requirements fully (100%) cover the deployed contracts?” to “Does the software function documentation fully (100%) cover the deployed contracts?” because many people do not really understand the word "requirements". Also added guidance to this question
3. Added guidance based on Comments to Code (CtC) ratio on the question “Are there sufficiently detailed comments for all functions within the deployed contract code?” Change the wording of the question from “Is it possible to trace software requirements to the implementation in code” to “Is it possible to trace from software documentation to the implementation in code” because many people do not really understand the word "requirements".
   Test
4. Added guidance based on Test to Code ratio (TtC) to the “Full test suite” is a good

Audits

1. Added words where audits do not cover economic issues and the specific impact of audits on private repos

0.5 -- 7 August 2020

Added % Guidance to "Does the code match a tagged version on a code hosting platform (GitHub, GitLab, etc.)?"

Added % Guidelines to "Code coverage (Covers all the deployed lines of code, or explains misses) (%)" in Testing

Added % Guidelines to "Is it possible to trace requirements to the implementation in code (%)"

0.4 -- 24 July 2020

General rebalancing of the scoring weights

Added Summary of the Process section

Changed Deployed code to "Executing Code Verification"

Changed Requirements to Documentation

Scoring weight for the "deployed code address(s) readily available?" from 10 to 30 because it is fundamentally important

Scoring weight for the "Does the code match a tagged version on a code hosting platform (GitHub, GitLab, etc.)?" from 10 to 20

Scoring weight for the "Is development software repository healthy)?" from 20 to 10

Changed the heading of Requirements to Documentation for better clarity for the reader.

Deleted "Are the requirements available publicly? Question as it added little value.

Scoring weight for the "Are there sufficiently detailed comments for all functions within the deployed contract code?" from 5 to 10 because is important

Scoring weight for the "Code coverage", "Scripts and instructions to run the tests" and "Packaged with the deployed code" from 10 to 5 for balancing

Changed the weight of Audit from 50 to 70 for balancing

0.3 -- June 2020

"Is development software repository healthy?" of "Deployed Code" changed from Y/N to %. The AAVE code was developed in a private repository that the auditor cannot view. The public repository was created just to display the final code. This makes the public repository appear unhealthy. But as they have a valid reason and the auditor is comfortable a valid repository exists but cannot be seen we needed something better than a binary Y/N. So we changed to % and changed the explanation.

0.2 -- June 2020

This is the initial version used for the first three Audits