A smart contract audit

is a time-boxed security-based code review on your smart contract or protocol. An auditor's goal is to find as many vulnerabilities as possible and educate the client on ways to improve the security of their codebase moving forward.

Smart contract auditors use manual and automated tools to find these vulnerabilities.

In this article, you'll learn why smart contract security reviews are important and why you should get one (or multiple) before deploying your smart contracts to production.

Here's the video related to this article:

https://www.youtube.com/watch?v=aOqhQvWhUG0

Why are smart contract audits important?

According to a research study byChainalysis, 2022 was the year the most value was stolen from smart contracts.Due to the immutability of the blockchain, once a smart contract is deployed, you can't change it, so you'd better get it right. The blockchain is an adversarial environment, and your protocol needs to be prepared for malicious users.But even more than saving your protocol from hacks, a smart contract audit can improve your developer's understanding of code, improving their speed and effectiveness of features moving forward.

Let's take a look at some of the benefits of smart contract security audits:

Benefits of a smart contract security review

• Enhance the security of your protocol and its users

by finding vulnerabilities

• Level up your engineering team knowledge

by learning and implementing state-of-the-art smart contract development best practices

• Establish trust with your users and the community

- Smart contract audits are vital in communicating maturity and safety to your users.

How does a smart contract audit work?

A smart contract security audit is a comprehensive process

. Smart contracts can include thousands, if not tens of thousands, of lines of code. Given this volume, even obvious issues can sometimes be missed. That's why more than a single audit is often required. Many protocols undertake a security journey that joins multiple audits, competitive audits, and Bug Bounty Programs.

Both testing tools and human auditors are essential for identifying errors and potential vulnerabilities in the existing code. Here is an overview of the smart contract security audit process.

Smart contract audit process

1. Security review price and timelines

To get a smart contract audit, a protocol can contact asmart contract security firm before or after its code is finished. Ideally, they reach out some time before so the auditor can have enough time to schedule them.

Once they reach out, the teams will discuss how long the audit will take based on the scope and code complexity. How long the audit will take depends on how many lines of code. A rough approximation of how long an audit takes depending on how many source lines of code you have can be later down in this article.

2. Commit hash, down payment, and start date

Auditors need to know exactly what code they are auditing and will use the commit hash of your repo to do so. Once your

code is ready and pushed on GitHub, the security company will usually ask you for the commit hash. Once finalized, you can reach a start date and finalize the price.

3. Run tests with tools

Once the audit begins and the auditors understand your codebase, they will begin using a set of smart contract security tools and automated tests. This is the initial step to identifying simple issues and concentrating on high-severity and more complex problems.

In this phase, the auditors will employ various methods, such as integration tests, static analysis, fuzz testing, and unit testing, to thoroughly examine the security of the codebase.

4. Manual review of code

While automated tests can detect basic and some advanced vulnerabilities in the codebase, uncovering more complex and "hidden" issues calls for manual intervention by a smart contract security researcher. By grasping the context and complexity of the code and cross-referencing the project specification and any supplementary documentation, auditors can identify deeper vulnerabilities.When an audit team analyzes the code

, it is important to use a mixture of manual and automated testing. This approach is vital to ensure that everything runs smoothly.

5. Initial smart contract audit report

After the initial smart contract security review

period, the auditors will provide an initial report to the protocol team. This smart contract audit report will include:

- Findings listed by severity, typically classified as High, Medium, or Low
- Informational, Non-critical, or Gas findings
- Suggestions for mitigation and potential solutions to the issues identified

Once the report is finalized, the mitigation phase will begin.

6. Mitigation

The protocol team will then have an agreed-upon time to address the vulnerabilities identified in the initial audit report. The duration can vary, often much shorter than the audit itself, but may be longer depending on the severity of the findings.

7. Final smart contract audit report

Following the protocol changes, the audit team will produce a final smart contract audit report focusing solely on the fixes to address the issues highlighted in the initial report. Ideally, the auditors and the protocol team will have had a positive experience and collaborate to ensure future security.

8. After the smart contract audit

We recommend acting on the smart contract audit report findings. Ignoring these warnings can expose vulnerabilities, which are often exploited.Furthermore, if you alter your codebase, this becomes unaudited code and should not be implemented, regardless of the size of the change. If you modify your code, consider having that section audited.Depending on the funds your protocol will secure, an additional audit may be worth considering.

How long does a smart contract audit take?

The duration of a smart contract security audit primarily depends on the size and complexity of the code

. An audit company with the right tools and expertise can typically make a comprehensive report within one to two weeks. However, auditing more extensive applications may require more time. Allocating sufficient time for a thorough security audit is crucial for your blockchain application's success.

How much does a smart contract audit cost?

The smart contract audit pricing is determined by the duration

, with costs varying greatly based on the size and complexity

of the codebase. Generally, smart contract auditors may charge anywhere from $5,000 to $60,000 per week

, which can increase depending on the protocol's size and complexity.

If you're considering launching a protocol, having your smart contracts audited by an [experienced auditing company

](https://blaize.tech/article-type/web3-security/top-smart-contract-audit-companies/)is a no-brainer

. These contracts execute financial transactions and are used for essential functions. Unlike other types of software, it's crucial to have bug-free code to avoid potential protocol and financial-breaking exploits.

How to get the most out of a smart contract audit

1. Write clear documentations

Providing a smart contract security team with ample context, documentation, and information about a given protocol is essential for their understanding. Ensuring anyone can easily comprehend your code

and its intended functionality is crucial. Since 80% of all bugs are due to business logic issues, auditors require a clear understanding of the protocol's expected operations more than the actual code itself.

2. Provide a robust test suite

Maintaining a comprehensive test suite that covers a significant portion of your codebase enables auditors to concentrate on issue identification rather than tool manipulation. Before an audit, incorporate fuzz testing unit tests

and run a smart contract security tool.

This approach can reduce your costs and minimize the time the auditing team spends reviewing your codebase and looking for surface-level issues.

3. Do an initial video walkthrough of the code

The first step in a smart contract audit should be a high-level video walkthrough. This walkthrough should explain your codebase, describe how the code is intended to function, and guide you where to find answers.

Conclusions - What is not a smart contract audit?

Remember, an audit does not guarantee that your code is bugs-free

. It's a part of your security journey where your team should continually strive to improve.

Regardless of an auditor's experience, there will always be instances where something is overlooked. If that unfortunate day comes, convene with your auditors on an emergency communication channel and devise a quick solution.

Even the most thoroughly audited protocols may benefit from insurance.

With this information, you should now have a solid understanding of the end-to-end smart contract audit process. Remembering that a smart contract audit is a security journey between the protocol and auditors is important. Maintaining a security-focused mindset is crucial, even after the audit is complete.

If you're looking for an audit, contact the Cyfrin team. And as always, stay safe out there!