A smart contract audit is a time-boxed security-based code review on your smart contract/web3 system. 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.

Auditors use a combination of manual and automated tools to find these vulnerabilities.

Why are smart contract audits so important?

According to a research study by Chainalysis, 2022 was the year the most value ever 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 so than just saving your protocol from hacks, an audit can improve your developer's understanding of code, improving their speed and effectiveness of features moving forward.

Additionally, there is an entire website dedicated to how many hacks happen, and we need to do our best to prevent that list from growing as a community.

Smart Contract Audit Benefits

- Find vulnerabilities
- Level-up developers
- Teach best practices and the most modern tooling

Often, one audit isn't enough. Many protocols go on a security journey that includes multiple audits and services like:

- Formal Verification
- Competitive Audits
- Bug Bounty Programs

We'll break these down in a future video.

Smart Contract Auditors

There are a lot of companies that offer smart contract auditing services, like:

- Cyfrin <- This is us!
- Trail of Bits
- Consensys Diligence
- Openzeppelin
- Sigma Prime
- SpearbitDAO
- MixBytes
- WatchPug
- Trust

Additionally, there are a lot of independent auditors that do great work as well.

Smart Contract Audit Process

A typical audit looks like this:

1. Price & Timeline
2. A protocol can reach out before or after their code is finished. Ideally, they reach out some time before so the auditor

can have enough time to schedule them.

3. Once they reach out, the teams will discuss how long the audit will take based on the scope and code complexity.
4. How long the audit will take depends on how many lines of code.A very rough approximation of how long an audit takes depending on how many source lines of code you have can be found here:
5. The duration sets the price, and at the time of recording, prices can range widely based on the different auditors. At the time of recording, a one-week-long audit can go anywhere from:
6. Duration: Price
7. 1 week: $5,000 - $100,000
8. Commit Hash, Down payment, Start Date
9. Auditors need to know exactly what code they are auditing and use the commit hash of your repo to do so. Once you have a commit hash, you can reach a start date and finalize the price.
10. Audit Begins
11. Then the audit starts! Your auditors will use every tool in their arsenal to find vulnerabilities in your code.
12. Initial Report
13. After the period ends, the auditors will give you an initial report that looks like this.
14. All their findings are listed by severity, usually in formatted into:
15. High
16. Medium
17. Low
18. Informational / Non-critical / Gas
19. Mitigation Begins
20. The protocol's team will then have an agreed-upon time to fix the vulnerabilities found in the initial audit report. Sometimes, depending on the severity of the findings, this may be long but is often much shorter than the audit itself.
21. Final Report
22. After the protocol makes the changes, the audit team will do a final audit report exclusively on the fixes made to address the issues brought up in the initial report.

And then, hopefully, the auditors and protocols have had a great experience and will work together to stay secure in the future!

How to get the most out of a smart contract audit

To get the most out of an audit, you should:

- Have clear documentation
- Robust test suite
- Ideally, including fuzz tests
- Code should be commented & readable
- Modern best practices followed
- A communication channel between developers and auditors
- Do an initial video walkthrough of the code

The most important part of the process, though is during the audit.

You want to think of you and your auditor as a team to get the best results out of your audit. One of the best ways to do this is to have a dedicated channel where auditors can ask questions to the developers.

Additionally, the more context, documentation, and information they can read, the better. Be sure it's easy for anyone to walk through your code and understand what it's supposed to do.

80% of all bugs are due to business logic issues, so the auditors need to understand what the protocol should do more than they should understand the actual code!

Having a modern test suite & tooling can also make it so auditors spend less time fidgeting with your tooling and more time finding issues.

A high-level video walkthrough of your code should be the first thing you and the auditors do together.

After the Audit

We highly encourage you to act on the recommendations of an audit report, we've seen too many protocols not take warnings seriously, and that be the attack vector that gets exploited.

Additionally, if you change your codebase, that is now unaudited code, and should not be pushed, no matter how small the change may be. If you change your code, you should highly consider getting that piece of code audited.

And often, depending on how much money your protocol will secure, you should consider getting another audit anyway!

What an audit isn't

Now here is the thing, an audit does not mean your code is bug-free. It's a security journey where your team should level up on security.

No matter how experienced an auditor or audit firm is, people at all levels of experience will miss something. On the sad day that happens, get together on an emergency communication channel with your auditors and figure out to remedy the situation quickly.

Insurance is often a good idea for even the most audited protocols.

So with that, now you have a good idea of the smart contract audit process end to end and what to expect. A smart contract audit is more of a security journey between the protocol and the auditors, and having a security-focused mindset doesn't end even after the audit.

If you're looking for an audit, be sure to contact theCyfrin team. And as always, stay safe out there!

According to a research study by Chainalysis, 2022 was the year the most value ever 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 so than just saving your protocol from hacks, an audit can improve your developer's understanding of code, improving their speed and effectiveness of features moving forward.

Additionally, there is an entire website dedicated to how many hacks happen, and we need to do our best to prevent that list from growing as a community.