## Audit Process

* Contact (Prepared Code-Email)
* Quote (Timeline)
* Audit (Commences)
* Report (Private)
* Fixes (Team Address)
* Publish– Optional (Examine Fixes & Update)

[Points: Clear +1, Formal +1 | MAX: 2/2]

## OpenZeppelin: Pre-audit/Standards [Checklist](https://blog.openzeppelin.com/follow-this-quality-checklist-before-an-audit-8cc6a0e44845/)

*Checklist Summary;*

* Choose a free software license.
* Build a strong and diverse team of core maintainers.
* Increase your bus factor: share knowledge and responsibilities.
* Choose a good leader.
* Write clean code.
* Enforce a consistent code style.
* Ensure 100% unit test coverage.
* Enforce green tests on all your pull requests.
* Design your iterative development and testing process.
* Publish your code.
* Write a good README.
* Document the functions of your public API.
* Document your protocol.
* Write the end-user documentation.
* Make sure that your dependencies can be trusted.
* Review known issues and keep an eye out for new ones.
* Use OpenZeppelin Contracts, the community-vetted standard for smart contract development.
* Build and care for your community.

[Points: Clear Pre-requisites/Standards +1 | MAX: 1/1]

## Audit Format

* **Introduction**

-[Project](https://augur.net/) & [Code](https://github.com/AugurProject/augur-core/tree/3b5a63d372d205a0214e3061293d5bca0fd5636a)

-Github: [Updates](https://github.com/AugurProject/augur-core/commit/7f3c79a5dd471a98df8f66a640902e063f15f796) & Commit [ID's](https://github.com/AugurProject/augur-core/commit/45e1afb7eb1a895d923c97fe01e068c772c583ef)

-[Full audit report](https://docs.google.com/document/d/1saSVpT2Ixd58q-DZlTtzfkNizuTTE4yVoGuWz_AatZM/edit)

* **Vulnerabilities & Issues**

1. -Critical Severity
2. -High Severity
3. -Medium Severity
4. -Low Severity

* **Notes**

-Additional commentary on the codebase.

* **Conclusion**

-Summary of report and issues found in the presented code. Any updates and fixes are addressed in the conclusion. Including, best practice recommendations, suggestions to reduce attack vectors.

* **Summary**

-Included overview of technical audits for the non-technical reader. ([Compound Finance audit summary](https://blog.openzeppelin.com/compound-finance-audit-summary/))

## Popular Reports

* [Augur](https://augur.net/) ([Core](https://blog.openzeppelin.com/augur-core-audit-244160d77c09/))
* [Solidity](https://soliditylang.org/) ([Compiler](https://blog.openzeppelin.com/solidity-compiler-audit-8cfc0316a420/))
* [Brave](https://basicattentiontoken.org/) ([BAT](https://blog.openzeppelin.com/basic-attention-token-bat-audit/))
* [Compound](https://compound.finance/) ([Protocol](https://blog.openzeppelin.com/compound-audit/))
* [MakerDAO](https://makerdao.com/en/) ([Critical Vulnerability](https://blog.openzeppelin.com/makerdao-critical-vulnerability/))
* [Centre](https://www.centre.io/) ([Token Minting Contracts](https://blog.openzeppelin.com/centre-token-minting-contracts-audit-6e723177d44b/))

[Points– Multiple Auditors +1, Industry Lead +1, Structure +1, Clarity +1 & Consistency +1 | MAX: 5/5]

## Contact

Website Links: [Audits](https://openzeppelin.com/security-audits/), [Blog](https://blog.openzeppelin.com/), [Reports](https://blog.openzeppelin.com/security-audits/), [Audit Request](https://openzeppelin.com/request/) & [Docs](https://docs.openzeppelin.com/openzeppelin/)

Twitter: [@OpenZeppelin](https://twitter.com/openzeppelin)

Github: [OpenZeppelin](https://github.com/openzeppelin)

Discord: [Public](https://discord.com/invite/EvUjsZdaaM)

[Points– Public Profiles; Transparency +1, Community Discord/Telegram/Reddit +1 | MAX: 2/2]

[**Points total: 10/10**]