Mimo DAO

Contract Audit Report

VER 1.2

7 May 2022

No. 2022050715201

Project Summary

1. Project Introduction

Mimo DAO is mainly a decentralized autonomous community DAO product. Users can obtain vePICO tokens by staking their tokens. The quantity is adjusted according to time weighting. Users can use their vePICO to conduct liquidity for different pools. The weight of mining is voted and changed in time. Use this to obtain corresponding rewards or continue to make secondary pledges for compound interest.

2. Audit Summary

Project Name	Mimo DAO	**Platform**	N/A
Token	N/A	**Token symbol**	N/A
Start date	12 Apr 2022	**Language**	Solidity and Vyper
End date	29 Apr 2022	**Website**	N/A
Github	https://github.com/mimoprotocol/mimo-dao-contracts/tree/4c70aca60fc5a87904a499c473f85399a643d04b	**whitepaper**	N/A

7 May 2022

3. Audit Scope

ID	File	SHA-256 checksum
contracts	ERC20PICO.sol	0765b1ab538a77d4f9b3e039c4b64db16e3528f8d397fcc5b013492e4024bac5
contracts	GaugeController.vy	14bca5587133962b6ee6ce9897ab1a1e5ef9dd45905b1beb932c75270c6e7457
contracts	VeBatchLocker.sol	649a9f2adcab102d9bdb416b1aa78df4d60a943caef971dfc6d1a43a689e8bf7
contracts	VestingMaster.sol	0b84bc0fb8e73d897b6dbff509b81efc96b0ec1e1af001e45591f3cdbb303a3f
contracts	VestingMinter.vy	13476de103d1045b45b9a977479fa4184ff99748e198d4984767729ba250616c
contracts	VotingEscrow.vy	6a8c92dfe6903a56849ba0a18c931b0a8a63aebd165bd71b38a4edb3013def35
contracts/gauges	LiquidityGaugeV3.vy	bc860000ba74b761595d56236f33091a32006a528d3f4642229a95c18884013a
contracts/interfaces	IVestingMaster.vy	df5174d37e539aafe96c7bc43ccc6f615b7923fad6f3dc6c74516f0e9c8ec290
contracts/interfaces	IVotingEscrow.vy	5befedc7899a0599d966b2ffe10f676646d81489d143268888437d5e0831857b

4. Code Structure

```
contracts

├─── ERC20PICO.sol
├─── GaugeController.vy
├─── VeBatchLocker.sol
├─── VestingMaster.sol
├─── VestingMinter.vy
├─── VotingEscrow.vy
├─── gauges
|    └─── LiquidityGaugeV3.vy
├─── interfaces
|    ├─── IVestingMaster.sol
|    └─── IVotingEscrow.sol
```

7 May 2022

Audit Report Summary

1. Audit Methods

The audit was conducted to gain a clear understanding of how the project was implemented and how it works. The audit team conducted in-depth research, analysis, and testing of the project code and collected detailed data. In this report, the audit team will list in detail each issue identified, where it is located, the root cause of the issue, and a description of the issue, and will recommend changes to the issue accordingly.

Audit methods	Static analysis, Manual Review

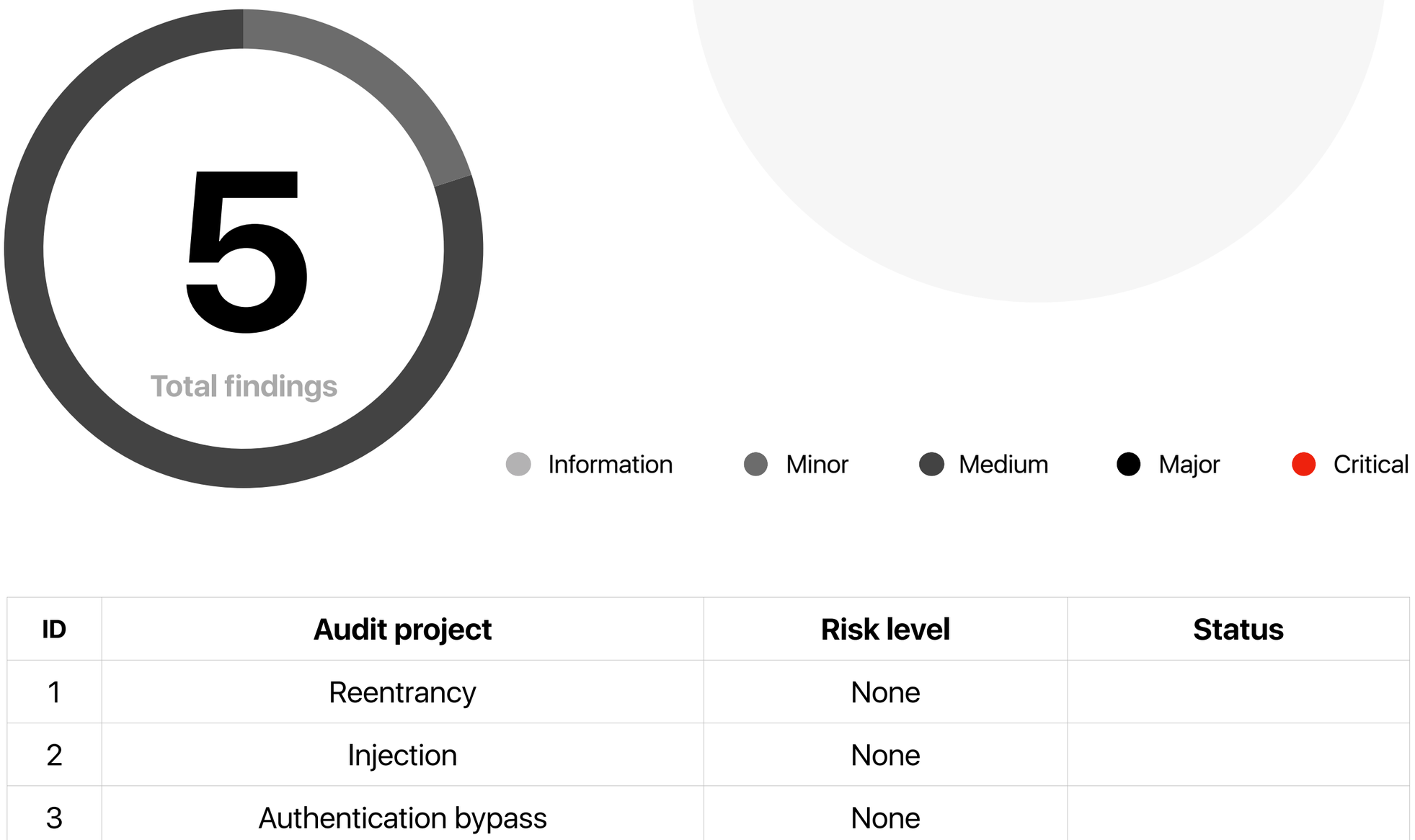
2. Audit Process

Steps	Operation	Description
1	Background	Read project descriptions, white papers, contract source code, and other relevant information the project team provides to ensure a proper understanding of project functions.
2	Automated testing	Scanning source code mainly with automated tools to find common potential vulnerabilities.
3	Manual reveiw	Engineers read the code line by line to find potential vulnerabilities.
4	Logical proofread	The engineer will compare the understanding of the code with the information provided by the project and check whether the code implementation is in line with the project white paper information.
5	Test case	Including test case design, test scope analysis, symbolic execution, etc.
6	Optimization items	Review of projects in terms of maintainability, safety, and operability based on application scenarios, deployment methods, and latest research results.

3. Risk Levels

Risk level	Issue description
Critical	Fatal risks and hazards that need to fixed immediately.
Major	Some high risks and hazards that will lead to related problems that must be solved
Medium	Some moderate risks and pitfalls may lead to potential risks that will eventually need to be addressed
Minor	There are low risks and hazards, mainly details of various types of mishandling or warning messages, which can be set aside for the time being
Information	Some parts can be optimized, such problems can be shelved, but it is recommended that the final solution

4. Audit Results



ID	Audit project	Risk level	Status
1	Reentrancy	None	
2	Injection	None	
3	Authentication bypass	None	
4	MEV Possibility	None	
5	Revert	None	
6	Race condition	None	
7	Insufficient Gas Griefing	Medium	Acknowledged
8	The major impact of flash loans	None	
9	Unreasonable economic model	None	
10	Predictable random numbers	None	
11	Voting rights management confusion	None	

ID	Audit project	Risk level	Status
12	Privacy leak	None	
13	Improper use of time on chain	None	
14	Improper codes in fallback function	None	
15	Improper identification	None	
16	Inappropriate opcode	None	
17	Inappropriate assembly	None	
18	Constructor irregularities	None	
19	Return value irregularity	None	
20	Event irregularity	Minor	Resolved
21	Keywords irregularity	None	
22	Not following ERC standards	None	
23	Irregularity of condition judgment	None	
24	Risk of liquidity drain	None	
25	Centralization Risk	Medium	Acknowledged
26	Logic change risk	None	
27	Integer overflow	None	
28	Improper function visiblity	None	
29	Improper initialization of variables	Medium	Resolved
30	Improper contract calls	None	
31	Variable irregularities	None	
32	Replay	None	
33	Write to Arbitrary Storage Location	None	
34	Honeypot logic	None	
35	Hash collision	None	
36	Improper logic in receiving awards	None	
37	Use the not recommended method	None	
38	Basic coding principles were not followed	None	
39	Third-party dependency risk	None	

* In the above table, if the status column is “**Acknowledged**”, the audit team has informed the project owner of the vulnerability. Still, the project owner has not made any changes to the vulnerability or has not announced to the audit team the progress of the changes to the vulnerability. If the status column is “**Resolved**”, the project owner has made changes to the vulnerability, and the audit team has confirmed the changes.

5. Risk and Modification Program

The following section provides detailed information about the risk items learned after the audit, including the type of risk, risk level, location of the issue, description of the problem, recommendations for changes, and feedback from the project owner.

Risk type	Insufficient Gas Griefing	**Risk level**	**Medium**
Location	Line 323	Contract file	LiquidityGaugeV3.vy
Description	When the user executes checkpoint to update the checkpoint dashboard information, it depends on the loop. If the update is not performed for a long time, the loop may cause gas exhaustion, transaction failure or high user cost.		
Recommedation	Deploy automatic scripts to update user information regularly.		
Update	-		

Risk type	Insufficient Gas Griefing	**Risk level**	**Medium**
Location	Line 175,198,238,268	Contract file	GaugeController.vy
Description	When calculating voting weight information and statistics, it is easy to cause gas exhaustion and transaction failure.		
Recommedation	Deploy automatic scripts to update user information regularly.		
Update	-		

Risk type	Centralization Risk	**Risk level**	**Medium**
Location	Line 158	Contract file	VestingMaster.sol
Description	Contract functions involving permission control do not have timelock mechanism or multi sign mechanism.		
Recommedation	Disperse the permissions of a single private key, and use timelock and multi sign mechanism.		
Update	The project plans to use a multi-signature and timelock mechanism, but currently not mentioned in the code.		

Risk type	Improper initialization of variables	**Risk level**	**Medium**
Location	Line 108	Contract file	VotingEscrow.vy
Description	The contract global variable migrate is not initialized, which leads the migrate function cannot be used.		
Recommedation	Add a setter function to the migrator variable.		
Update	Resolved		

Risk type	Event irregularity	**Risk level**	**Minor**
Location	L374	Contract file	VotingEscrow.vy
Description	In "Only owner can deposit for others", the owner does not clearly refer to the contract admin or the owner of the parameter _wallet.		
Recommedation	If owner refers to the contract admin, assert will not work. If it refers to the owner of the parameter _wallet, please modify the prompt string.		
Update	Resolved		

6. Recommandation

N/A

Disclaimer

i. This audit report focuses only on the types of audits identified in the final report issued. Other unknown security vulnerabilities are not part of this audit, and we do not accept responsibility for them.

ii. We shall only issue an audit report based on an attack or vulnerability that existed or occurred before the issuance of the audit report. We cannot determine the likely impact on the security posture of our projects for new attacks or vulnerabilities that may exist or occur in the future, and we are not responsible for them.

iii. The security audit analysis and other elements of our published audit report shall be based solely on documents and materials (including, but not limited to, contract codes) provided to us by the Project Party before the release of the audit report. Such documents and materials shall not be untrue, inaccurate, uninformative, altered, deleted, or concealed, and if the documents and materials provided by the Project Party are false, inaccurate, uninformative, changed, deleted or hidden, or if the documents and materials provided by the Project Party are untrue, inaccurate, uninformative, altered, deleted or concealed, or if the documents and materials provided by the Project Party are uninformative, uninformative, altered, deleted or hidden. If the records and information provided by the Project Party are untrue, inaccurate, uninformative, altered, deleted, or concealed, or if changes to such documents and information are made after the issuance of the audit report, we shall not be liable for any loss or adverse effect arising from any inconsistency between the reflected and actual conditions.

iv. The Project Parties are aware that our audit report is based on documents and information provided by the Project Parties and relies on the technology currently available. However, due to the technical limitations of any organization, there is a possibility that our audit report may not fully detect all risks. Our audit team encourages the project development team and any interested parties to conduct subsequent testing and audits of the project.

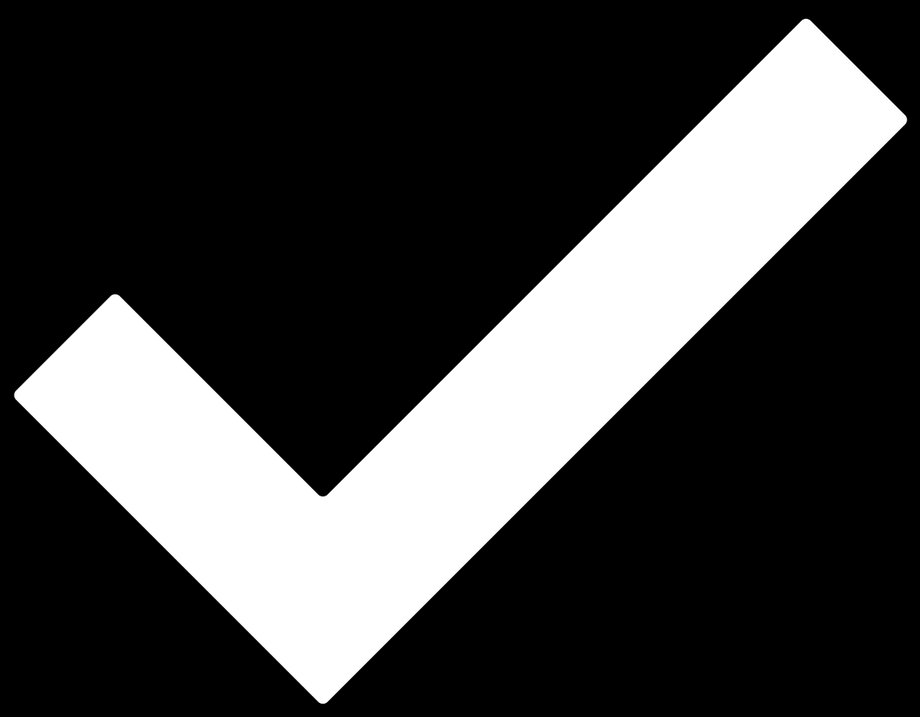
v. The project owner warrants that the project for which we are engaged to provide audit or testing services is legal, compliant, and does not violate applicable laws. The audit report is for the project owner's reference only, and the contents, manner of obtaining, use of, and any services or resources involved in the audit report shall not be relied upon for investment, tax, legal, regulatory, or advisory purposes of any kind, and we shall not be liable therefor. The Project Party shall not refer to, quote, display, or send the Audit Report in whole or in part to any third party without our prior written consent. The Project Party shall bear any loss or liability arising from that place. We assume no responsibility for any reliance on or use of the audit report for any purpose.

vi. This audit report does not cover the compiler of the contract or any areas beyond the programming language of the Smart Contract. The risk and liability of the audited Smart Contract arising from references to off-chain information or resources is the sole responsibility of the project party.

vii. Force Majeure. Force majeure means an unforeseen event whose occurrence and consequences cannot be avoided and cannot be overcome by the parties at the time of entering into the contract, including but not limited to natural disasters such as war, typhoon, flood, fire, earthquake, tidal wave, lightning, natural disaster, strike, nuclear explosion, epidemic and other unforeseen events such as changes in laws, regulations and policies and governmental acts, whose occurrence and consequences cannot be prevented or avoided, and which contains, affects or delays the performance by either party of all or part of its obligations under the contract.

viii. Suppose either party believes that the occurrence of force majeure affects the performance of its obligations under this Agreement. In that case, it shall promptly notify the other party and, depending on the extent of the effect of the event on the performance of the Agreement; the parties shall consult to determine whether to terminate the Agreement or partially relieve itself of its obligations to perform the Agreement, or to extend the performance of the Agreement.

ix. In force majeure, neither party shall be deemed in breach or non-performance of its obligations under this Agreement. Any financial commitments existing before the event shall not be affected, and the project party shall make payment for work performed by us.



Passed.

Date	7 May 2022
Audit Team	歐科雲鏈

The purpose of this audit is to review the voting staking and management functions of the Mimo DAO project based on Solidity and Vyper languages, study its design and architecture, discover potential security risks, and try to find possible loopholes.