Aarna (AtvWrappedBoosterTL)

Smart Contract Audit Report

19th August 2025

FAILSAFE

Table of Contents

Executive Summary

The objective of this project is to perform a comprehensive security and functionality audit of the Aarna Protocol smart contracts. Aarna is a DeFi protocol that manages user investments, withdrawals, and yield accrual through a sophisticated vault structure with advanced rebalancing strategies, strict access control, and upgradeable architecture. Given the high value and irreversible nature of blockchain transactions, any vulnerability in these contracts could result in significant financial loss and reputational damage. This audit aims to identify critical, major, and minor issues, as well as provide optimization recommendations to enhance code efficiency, maintainability, and transparency. This audit covers only the AtvWrappedBoosterTL that will be used for the Aarna Pendle integration.

Throughout the audit process, the Aarna team demonstrated exceptional commitment to security, responding to findings with remarkable speed and implementing fixes within hours of receiving critical vulnerability reports. Their proactive security posture and rapid response capabilities reflect a mature security culture and strong operational discipline. The team's ability to quickly validate, acknowledge, and remediate security issues showcases their technical expertise and dedication to maintaining the highest security standards.

Project Details

Project	Aarna Protocol
URL	hhttps://www.aarna.ai/
Source Code	https://github.com/pcode-ai/afi-timelock/
Initial Commit	41c5fcfada87d2d792de1bcd8ce3f579d9c2657b
Final Commit	bdbe382e61b8acd3aea0c253124cf065079a2bf5
Timeline	Initial Report - 9th August 2025 - 10th August 2025
	Final Report - 10th August 2025 - 19th August 2025

Structure & Organization of Audit Report

Issues are tagged as “Open”, “Acknowledged”, “Partially Resolved”, “Resolved” or “Closed” depending on whether they have been fixed or addressed.

- Open: The issue has been reported and is awaiting remediation from developer team.
- Acknowledged: The developer team has reviewed and accepted the issue but has decided not to fix it.
- Partially Resolved: Mitigations have been applied, yet some risks or gaps still remain.
- Resolved: The issue has been fully addressed and no further work is necessary.
- Closed: The issue is deemed no longer pertinent or actionable.

Furthermore, the severity of each issue is written as assessed by the risk of exploitation or other unexpected or otherwise unsafe behavior:

Critical	The issue affects the Smart Contract in such a way that funds may be lost, allocated incorrectly, or otherwise result in a significant loss.
High	The issue affects the ability of the Smart Contract to compile or operate in a significant way.
Medium	The issue affects the ability of the Smart Contract to operate in a way that doesn’t significantly hinder its behavior.
Low	The issue has minimal impact on the Smart Contract’s ability to operate.
Info	The issue is informational in nature and does not pose any direct risk to the Smart Contract’s operation.

Project Goals

1. Security Assurance

Ensure the Aarna smart contracts are free of critical vulnerabilities and follow industry-standard security best practices (e.g., SWC Registry, OpenZeppelin guidelines).

2. Functional Correctness

Verify that the contracts behave as intended according to the Aarna protocol specification, including proper handling of edge cases and failure modes for investment, withdrawal, and yield accrual.

3. Gas Optimization

Review the contracts for inefficient logic or high gas-consuming operations and provide suggestions to optimize transaction costs for users and protocol operators.

4. Access Control & Privileges

Analyze the roles and permissions within the contracts to prevent unauthorized actions, privilege escalations, or accidental lockouts, with a focus on the allowlist, admin roles, and pausing mechanisms.

5. Upgradability & Maintainability

Evaluate the contracts' upgradeability and maintainability, especially regarding proxy patterns, modular architecture, and future extensibility.

6. Compliance & Documentation

Ensure that the contracts are well-documented, follow Solidity development conventions, and provide clear, accessible documentation for future developers and auditors.

7. Reporting & Remediation Guidance

Deliver a detailed audit report categorizing all findings and recommending steps for remediation, along with a final verification round post-fix to ensure all issues are addressed.

Audit Methodology

FailSafe employs a multi-layered approach to Smart Contract security audits:

Threat Modelling: We identify critical assets, enumerate potential threats, assess vulnerabilities, and prioritize risks based on severity and impact.

Manual Code Review: Our experts conduct a detailed, line-by-line review of the code, analyzing business logic, access controls, gas efficiency, and external dependencies.

Functional Testing: Using frameworks like Hardhat and Foundry, we perform comprehensive functional and integration tests to ensure correct and secure Smart Contract behavior.

Fuzzing & Invariant Testing: Advanced techniques such as fuzzing and invariant testing are used to uncover hidden vulnerabilities and verify Smart Contract consistency under diverse scenarios.

Edge Case Analysis: We rigorously test for extreme inputs, exception handling, concurrency, and non-standard scenarios to ensure robust Smart Contract performance.

Reporting & Recommendations: Our reports clearly describe each issue, its impact, location, root cause, and provide actionable remediation steps and best practice guidelines.

Remediation Support: We work closely with your team to implement and validate fixes, followed by a final assessment to confirm all issues are resolved.

FailSafe's process ensures your Smart Contracts are secure from initial deployment through ongoing operation, providing proactive and comprehensive protection.

In-scope Files

- contracts/AtvWrappedBoosterTL.sol

Out of Scope

- All files and subdirectories under any mockcontracts/ directory
- Any file with "mock" in its filename (e.g., AFiExchangeMock.sol)
- Any test, migration, or deployment scripts

Summary of Findings

Severity	Total	Open	Acknowledged	Partially Resolved	Resolved	Closed
Critical	-	-	-	-	-	-
High	-	-	-	-	-	-
Medium	1	-	-	-	1	-
Low	1	-	-	-	1	-
Info	-	-	-	-	-	-
Total	2	0	0	0	2	0

#	Findings	Severity	Status
1	NAV Mismatch and Underflow Risk in Withdraw	Medium	Resolved
2	Approval Order Logic Issue	Low	Resolved

Finding 1: NAV Mismatch and Underflow Risk in Withdraw

Severity: Medium

Status: Resolved

Source: AtvWrappedBoosterTL.sol (deposit, withdraw, totalAssets, calculateNAV, convertToAssets)

Description:

`totalStaked` is updated with gross deposited underlying tokens, but the contract holds ATV vault shares with dynamic NAV. This causes `totalAssets()` to not reflect true value if vault NAV changes. Additionally, on withdraw, if NAV has increased (e.g., due to yields), computed `assets > totalStaked`, causing `totalStaked -= assets` to underflow and revert (preventing legitimate withdrawals).

Impact:

- Incorrect TVL reporting if NAV fluctuates.
- Withdraw reverts on underflow if yields make assets > totalStaked (DoS on user withdrawals).
- Misleads users; medium impact on functionality and trust.

Code:

```
// Deposit updates totalStaked with gross assets (line 254)
totalStaked += assets;

// totalAssets returns totalStaked without NAV adjustment (line 418)
function totalAssets() public view virtual override returns (uint256) {
    return totalStaked;
}

// Withdraw subtracts computed assets (line 541)
totalStaked -= assets;  // Underflows if assets > totalStaked due to NAV increase

// But calculateNAV uses dynamic vault TVL (line 224)
assetNAV = (IAFiStorage(atvStorage).calculatePoolInUsd(vault) * UNIT_NAV) / supply;

// convertToAssets uses current NAV (line 580)
uint256 assets = convertToAssets(shares);  // May be > original due to yields
```

Proof of Concept:

1. Deposit 1000 USDC: totalStaked += 1000.

2. Vault NAV increases 10%: Actual value ~1100, computed assets=1100 on withdraw (correctly using `_navMath` with current NAV).
3. Withdraw attempts totalStaked -= 1100 (from 1000) -> underflow revert (user can't withdraw, despite correct assets calc).
4. `totalAssets()` returns 1000 (stale, ignores yields).

Clarification Note: The assets amount is correctly computed using `_navMath` and current NAV (lines 588-592), ensuring users would get the adjusted value if the function succeeds. However, the underflow in totalStaked subtraction (line 541) reverts the transaction, preventing payout.

Remediation:

Compute totalAssets dynamically: return `_convertToAssets(_sBal(address(ATV_VAULT)), Math.Rounding.Floor)`. For withdraw, remove or adjust totalStaked subtraction, or sync it with the current NAV before subtracting.

Developer Response:

Fix addressed in commit hash: bdbe382e61b8acd3aea0c253124cf065079a2bf5

Auditor Response:

Verified the fix.

Finding 2: Approval Order Logic Issue

Severity: Low

Status: Resolved

Source: AtvWrappedBoosterTL.sol (deposit)

Description:

In the `deposit` function (lines 492-505), the contract calls `token.approve(vault, assets)` before calling `SafeERC20.safeTransferFrom(token, msg.sender, address(this), assets)`. This creates a logical inconsistency where the contract approves spending of tokens it doesn't possess yet.

Impact:

Low impact - Function executes successfully but has a logical inconsistency. Code quality issue that violates the standard pattern of "approve what you have".

Code:

```
1  token.approve(vault, assets);           // :x: APPROVES BEFORE TOKENS EXIST!
2  SafeERC20.safeTransferFrom(token, msg.sender, address(this), assets);  // :
       white_check_mark: TOKENS ARRIVE HERE
3  ATV_VAULT.deposit(assets, UNDERLYING); // :white_check_mark: THEN DEPOSIT TO
       VAULT
```

Remediation:

Reorder to approve after receiving tokens.

Developer Response:

We have reordered the approve and transferFrom calls to fix the logical inconsistency. Fix hash: bdbe382e61b8acd3aea0c253124cf065079a2bf5

Auditor Response:

Verified the fix.

Disclaimer

This audit report (“Report”) is provided by FailSafe (“Auditor”) for the exclusive use of the client (“Client”). The audit scope is limited to a technical review of the Smart Contract code supplied by the Client. This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you (“Customer” or the “Company”) in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without FailSafe’s prior written consent in each instance.

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts FailSafe to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. FailSafe’s position is that each company and individual are responsible for their own due diligence and continuous security. FailSafe’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by FailSafe is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, FAILSAFE HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, FAILSAFE SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, FAILSAFE MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE.

WITHOUT LIMITATION TO THE FOREGOING, FAILSAFE PROVIDES NO WARRANTY OR DISCLAIMER UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER FAILSAFE NOR ANY OF FAILSAFE'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. FAILSAFE WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT FAILSAFE'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST FAILSAFE WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF FAILSAFE CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST FAILSAFE WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.