ASSURE DEFI®

THE VERIFICATION GOLD STANDARD

SECURITY ASSESSMENT REPORT

NAME:	AURK
STATUS:	PASS
DATE:	12/01/2025

ASSURE DEFI®

Risk Analysis

Vulnerability summary

Classification	Description
🔴 High	Vulnerabilities that can lead to **loss or theft of funds**, **permanent locking of assets**, **unauthorized minting/burning**, **protocol insolvency**, or **full control of the contract or protocol**. These issues are typically **exploitable on-chain** and require immediate remediation.
🟠 Medium	Vulnerabilities that **weaken protocol security or trust assumptions** but do not directly enable immediate loss of funds under normal conditions. Exploitation may require **specific conditions, privileged roles, or external failures**.
🟡 Low	Issues that have **limited direct impact** on funds or protocol integrity but may cause **unexpected behavior**, **reduced resilience**, or **future exploitability** if combined with other weaknesses.
🟢 Informational	Findings that **do not represent security vulnerabilities**, but highlight **code quality, clarity, maintainability, or best-practice improvements** that may enhance long-term safety and auditability.

SCOPE

Target Code And Revision

Project	Assure
Codebase	aurk_contract.zip [SHA256]: 71a75e326f05ee76e4741785a105d8c17a5717871ff2f4cebdf8ce9664555e91
Audit Methodology	Static, Manual

Detailed Technical Report

HIGH

No high issues were found.

MEDIUM

1. Swapback DoS via “Maximum swaps per block” guard

Location:

_exchangeTokensForEth()

Issue:

Whenever a sell triggers a token-to-ETH swap (to == uniswapV2Pair and contractTokenBalance > _minSwapTokens), this guard limits swaps to two per block.

The third swap in the same block reverts the entire transaction, which includes the user’s sell.

This creates a griefing vector: anyone can make two small swap-triggering sells at the start of a block, then block all subsequent sells in that block.

This is deterministic, inexpensive, and repeatable (especially for MEV actors).

Result: legitimate users experience failed sells, and liquidity behavior becomes unpredictable.

Recommendation:

Replace the revert condition with a non-reverting guard:

```
if (block.number == _lastSwapBlock) {
    if (_swapCount >= 2) return; // skip swap, don't revert
    _swapCount++;
} else {
    _lastSwapBlock = block.number;
    _swapCount = 1;
}
```

Also introduce an inSwap boolean lock to prevent recursive calls instead of per-block limits.

2. Unbounded Slippage in Swapback (minOut = 0)

Location:

_exchangeTokensForEth()

Issue:

The swapback accepts any ETH output, even near-zero, allowing:

- MEV sandwiching
- Price manipulation immediately before swapback
- Long-term value leakage from holders

While not a direct fund-theft vector, it exposes the protocol to systematic economic loss during fee conversions.

Recommendation:

Enforce a minimum output based on expected reserves:

```
uint[] memory amounts = router.getAmountsOut(tokenAmount, path);
uint minOut = (amounts[1] * 90) / 100; // 10% slippage
```

LOW

1. Missing Transfer Event for Taxed Tokens

Location:

_executeTokenTransfer()

Issue:

Only the post-tax transfer emits a Transfer event.

The fee portion transferred to the contract is not emitted, causing:

- Incorrect indexing
- Analytics inconsistencies
- Integration issues

Recommendation:

Emit a second Transfer event for the tax amount:

```
emit Transfer(from, address(this), taxAmount);
```

INFORMATIONAL

No informational issues were found.

Technical Findings Summary

Findings

Vulnerability Level	Total	Pending	Not Apply	Acknowledged	Partially Fixed	Fixed
High	0					
Medium	2					
Low	1					
Informational	0					

Assessment Results

Score Results

Review	Score
Global Score	**90/100**
Assure KYC	Not completed
Audit Score	90/100

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 84 Points for a higher standard, if a project does not attain 85% is an automatic failure. Read our notes and final assessment below. The Global Score is a combination of the evaluations obtained between having or not having KYC and the type of contract audited together with its manual audit.

Audit PASS

Following our comprehensive security audit of the token contract for the **AURK** project, the project did **meet the necessary criteria** required to pass the security audit.

Disclaimer

Assure Defi has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocating for the Project, and users relying on this report should not consider this as having any merit for financial Token in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies. All information provided in this report does not constitute financial or investment in Token, nor should it be used to signal that any person reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided ‘as is, and Assure Defi is under no covenant to audit completeness, accuracy, or solidity of the contracts. In no event will Assure Defi or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report. The assessment of Tokens provided by Assure Defi are subject to dependencies and are under continuing development. You agree that your access or use, including but not limited to any Tokens, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The Token may access, and depend upon, multiple layers of third parties.