SMART CONTRACT AUDIT

ZOKYO.

August 15th 2022 | v. 1.0

PASS

Zokyo Security has concluded that this smart contract passes security qualifications to be listed on digital asset exchanges.

TECHNICAL SUMMARY

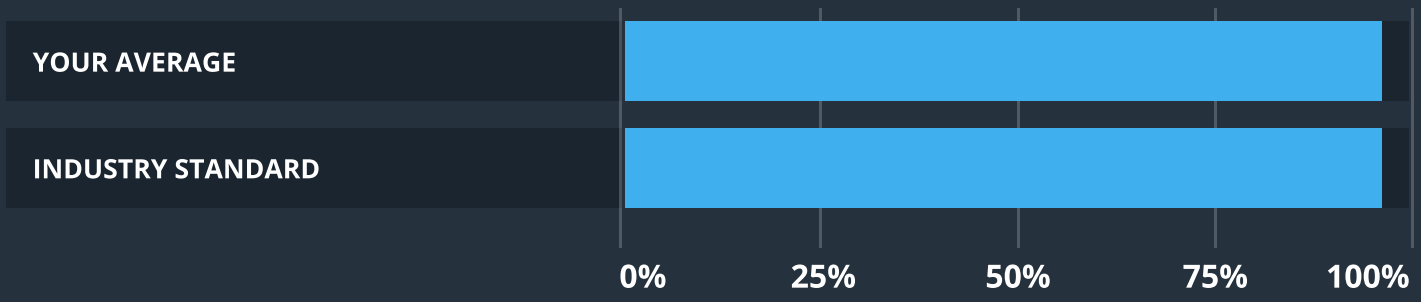
This document outlines the overall security of the IPOR smart contracts, evaluated by Zokyo's Blockchain Security team.

The scope of this audit was to analyze and document the IPOR smart contract codebase for quality, security, and correctness.

Contract Status

There were no critical issues found during the audit. (See Complete Analysis)

Testable Code



The 98% of the code is testable, which corresponds the standard of 95%.

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the contract, rather limited to an assessment of the logic and implementation. In order to ensure a secure contract that's able to withstand the Ethereum network's fast-paced and rapidly changing environment, we at Zokyo recommend that the IPOR team put in place a bug bounty program to encourage further and active analysis of the smart contract.

TABLE OF CONTENTS

AUDITING STRATEGY AND TECHNIQUES APPLIED

The Smart contract's source code was taken from the IPOR repository.

Repository - https://github.com/IPOR-Labs/ipor-protocol/commit/2a7cf870657f6ea0f7a356df79d7a60d5a3d2713

Last commit - 2a7cf870657f6ea0f7a356df79d7a60d5a3d2713

Within the scope of this audit, Zokyo auditors have reviewed the following contract(s):

- Milton.sol
- MiltonDai.sol
- MiltonInternal.sol
- MiltonStorage.sol
- MiltonUsdc.sol
- IporSwapLogic.sol
- SoapIndicatorLogic.sol
- Joseph.sol
- JosephDai.sol
- JosephInternal.sol
- AmmMiltonStorageTypes.sol
- AmmMiltonTypes.sol
- MiltonSpreadInternal.sol
- MiltonSpreadModel.sol
- MiltonSpreadModelDai.sol
- MiltonSpreadModelUsdc.sol
- MiltonSpreadModelUsdt.sol
- IporOracleFacadeDataProvider.sol
- MiltonFacadeDataProvider.sol
- CockpitDataProvider.sol
- IporErrors.sol
- IporOracleErrors.sol
- JosephErrors.sol
- MiltonErrors.sol
- MocksErrors.sol
- StanleyErrors.sol
- Constants.sol
- PaginationUtils.sol
- IporMath.sol
- IporOracle.sol
- IpToken.sol
- IvToken.sol
- IporOwnable.sol
- IporOwnableUpgradeable.sol
- Stanley.sol
- StanleyDai.sol
- StanleyUsdc.sol
- StanleyUsdt.sol
- IpToken.sol IvToken.sol
- StrategyAave.sol
- StrategyCompound.sol
- StrategyCore.sol

AUDITING STRATEGY AND TECHNIQUES APPLIED

Throughout the review process, Zokyo Security ensures that the contract:

- Implements and adheres to the existing standards appropriately and effectively;
- The documentation and code comments match the logic and behavior;
- Distributes tokens in a manner that matches calculations;
- Follows best practices in efficient use of resources, without unnecessary waste;
- Uses methods safe from reentrance attacks;
- Is not affected by the latest vulnerabilities;
- Meets best practices in code readability, etc.

Zokyo's Security Team has followed best practices and industry-standard techniques to verify the implementation of IPOR smart contracts. To do so, the code is reviewed line-by-line by our smart contract developers, documenting any issues as they are discovered. Part of this work includes writing a unit test suite using the Truffle testing framework. In summary, our strategies consist largely of manual collaboration between multiple team members at each stage of the review:

1	Due diligence in assessing the overall code quality of the codebase.	3	Testing contract logic against common and uncommon attack vectors.
2	Cross-comparison with other, similar smart contracts by industry leaders.	4	Thorough manual review of the codebase, line by line.

EXECUTIVE SUMMARY

There were no critical issues found during the audit. All the mentioned findings may have an effect only in case of specific conditions performed by the contract owner.

Contracts are well written and structured. The findings during the audit have no impact on contract performance or security, so it is fully production-ready.

Despite the fact, the expected logic is managing all vestings by the owner, it should be careful with parameters to avoid mistakes during the vesting process.

STRUCTURE AND ORGANIZATION OF DOCUMENT

For easier navigation, sections are arranged from most critical to least critical. Issues are tagged “Resolved” or “Unresolved” depending on whether they have been fixed or addressed. The issues that are tagged as “Verified” contain unclear or suspicious functionality that either needs explanation from the Customer’s side or is an issue that the Customer disregards as a problem. 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 contract in such a way that it can lead to a significant loss, funds may be lost or allocated incorrectly.

High

The issue affects the ability of the contract to compile or operate in a significant way.

Medium

The issue affects the ability of the contract to operate in a way that doesn’t significantly hinder its behavior.

Low

The issue has minimal impact on the contract’s ability to operate.

Informational

The issue has no impact on the contract’s ability to operate.

COMPLETE ANALYSIS

SYSTEM OVERVIEW

The core components of the IPOR Protocol are the Ipor Index, Liquidity Pools, AMM and Ipor Oracle. During the initial assessment of the protocol it has been discovered that at the center of these components is the price oracle and the price feeds it exposes. In most DeFi protocols, Oracles play an important role in securing the funds deposited within liquidity pools. After analyzing the oracle usage throughout the project, it has been established that further clarifications should be made. As such, Zokyo team engaged with the Ipor team over video call to discuss this component and the sources data is fed from.
It has been concluded that the smart contract implementation and how it's used throughout the components that consume feeds is correct and meets the set goals. After engagement with the Ipor team a conclusion has been reached regarding the Oracle long-term design and implementation. It has also been concluded that the current form of implementation, both on-chain and off-chain, is sufficient for the requirements specified by the Ipor team. Different proposals have been made regarding the centralized nature of the oracle and how feeds could be disrupted due to external/off-chain technical issues. It has been concluded that current existing oracle solutions, such as ChainLink, don't fully meet the requirements regarding composability and gas costs. So the decision has been made by the Ipor team to maintain the current solution and after ensuring a stable deployment and setup of the protocol, to gradually transition to a more decentralized approach. Ipor presented their design for the oracle following a review of resources requested from the Zokyo team. Although not in the scope of this report, support has been provided.
The Ipor protocol is a complex set of contracts and as such, to mitigate possible issues in the future or the need to accommodate new features, all contracts use the Oppenzeppelin's implementation of Universal Upgradeable Proxy Pattern (UUPS EIP-1822) for upgradeability. This is correctly implemented but no plans for governance have been communicated to the Zokyo team.
During the audit process the Ipor team found issues/optimizations which were discussed and fixed in pull requests reviewed by Zokyo. Some of the issues/optimizations were found by Zokyo and forwarded. These also got fixed and reviewed so are not part of this report.

COMPLETE ANALYSIS

FINDINGS SUMMARY

№	TITLE	RISK
1	Multiple external calls are executed in the same transaction (MiltonInternal)	Low
2	Multiple external calls are executed in the same transaction (StrategyAave)	Low
3	Incorrect balance assertion (MiltonInternal)	Informational
4	Incorrect balance assertion (Joseph)	Informational
5	Redundant usage of SafeMath (IvToken)	Low
6	Variable shadowing	Informational
7	Logical operator gas optimization	Informational

COMPLETE ANALYSIS

LOW | UNRESOLVED

Multiple external calls are executed in same transaction

In contract MiltonInternal, at line 348, there's an external call performed after another external call that queries the Ipor price oracle for the accruedIbtPrice. There are no checks for the returned value of the oracle, which can lead to undefined behavior if the oracle price feeds were not updated or the feeds are corrupted. In the current implementation, with the codebase of the Oracle being maintained by the Ipor team, this is not a problem. But given the oracle only defines an interface, and following discussions for the long-term goals of the oracle, this might change and the price feeds source might not be under the team's control.

Recommendation:
Refactor the flow such as the values returned by the oracle are taking into consideration the potential vulnerabilities mentioned above.

LOW | RESOLVED

Multiple external calls are executed in the same transaction

In contract StrategyAave at line 74, there's an external call performed that depends on another external call result. The first call retrieves the address of the lending pool for a certain asset and then queries the lending pool for its reserves data. Given the LendingPoolAddressProvider is a contract deployed by a 3rd party this could return invalid data and result in undefined behavior.

Recommendation:
Add a require check for zero address before querying the Aave lending pool to prevent undefined behavior.

INFORMATIONAL | ACKNOWLEDGED

Incorrect balance assertion

In contract MiltonInternal at line 328, in function _getAccruedBalance the liquidityPool balance is checked before returning the accruedBalance. The statement checks for greater than or equal to 0 balances, which is incorrect because for a 0 balance it would not revert.

```
require(liquidityPool >= 0, MiltonErrors.LIQUIDITY_POOL_AMOUNT_TOO_LOW);
accruedBalance.liquidityPool = liquidityPool.toUint256();
```

Recommendation:
Check the result returned by the function for the case when liquidityPool is 0 to avoid getting undefined behavior because of accruedBalance being 0.

INFORMATIONAL | ACKNOWLEDGED

Incorrect balance assertion

In contract Joseph at line 72, in function _calculateExchangeRate the balance is checked before calculating and returning the exchange rate. The statement checks for greater than or equal to 0 balances, which is incorrect because for a 0 balance it would not revert.

```
int256 balance = milton.getAccruedBalance().liquidityPool.toInt256() - soap;
require(balance >= 0, MiltonErrors.SOAP_AND_LP_BALANCE_SUM_IS_TOO_LOW);
```

Recommendation:
Check the result returned by the function for the case when balance is 0 to avoid getting undefined behavior because of exchangeRate being 0.

LOW | RESOLVED

Redundant usage of SafeMath

In contract IvToken at line 13, there's a using statement for uin256 involving SafeMath. Given all the contracts use Solidity 0.8.14 the SafeMath library is redundant, as in Solidity >=8.0.0 there can be no under/overflow.

Recommendation:
Remove the using statement for uin256 and the SafeMath library import.

INFORMATIONAL | RESOLVED

Variable shadowing

In contract MiltonStorage there are multiple instances of variable shadowing. It occurs in functions with named return types which are then redeclared inside the function body. It is present at lines 182, 203 and 235

Recommendation:
Remove duplicate declarations

Logical operator gas optimization

Milton -> 208, 222, 280, 379, 500, 672, 701, 796, 814
MiltonStorage -> 172, 193, 219, 295, 419, 432, 448, 487, 766, 788
SoapIndicatorLogic -> 80
Joseph -> 76, 85, 99, 123, 130, 187
JosephInternal -> 68, 120
MiltonSpreadModel -> 58, 76
MiltonFacadeProvider -> 116
IporMath -> 33
IporOracle -> 77, 95, 179, 210
lpToken -> 52, 58
lvToken -> 48, 54
Stanley -> 85, 120, 259, 452
StrategyCompund -> 135

In contracts above, for comparison between unsigned integers and the value 0 the “!=” operator was used. Based on the fact that all the variables are unsigned integers, comparison could be done with the ">” operator with the same result. Using the “>” operator the gas usage is 6x cheaper for this particular operation.

Recommendation:
Replace all comparison operators “!=” with “>”, as is described above.

	Milton.sol	MiltonDai.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	MiltonInternal.sol	MiltonStorage.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	MiltonUsdc.sol	IporSwapLogic.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	SoapIndicatorLogic.sol	Joseph.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	JosephDai.sol	JosephInternal.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	AmmMiltonStorageTypes.sol	AmmMiltonTypes.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	MiltonSpreadInternal.sol	MiltonSpreadModel.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	MiltonSpreadModelDai.sol	MiltonSpreadModelUsdc.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	MiltonSpreadModelUsdt.sol	IporOracleFacadeDataProvider.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	MiltonFacadeDataProvider.sol	CockpitDataProvider.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	IporErrors.sol	IporOracleErrors.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	JosephErrors.sol	MiltonErrors.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	MocksErrors.sol	StanleyErrors.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	Constants.sol	PaginationUtils.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	IporMath.sol	IporOracle.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	IpToken.sol	IvToken.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	IporOwnable.sol	IporOwnableUpgradeable.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	Stanley.sol	StanleyDai.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	StanleyUsdc.sol	StanleyUsdt.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	IpToken.sol	IvToken.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

	StrategyAave.sol	StrategyCompound.sol
Re-entrancy	Pass	Pass
Access Management Hierarchy	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass
Unexpected Ether	Pass	Pass
Delegatecall	Pass	Pass
Default Public Visibility	Pass	Pass
Hidden Malicious Code	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass
External Contract Referencing	Pass	Pass
Short Address/Parameter Attack	Pass	Pass
Unchecked CALL Return Values	Pass	Pass
Race Conditions/Front Running	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass
Floating Points and Precision	Pass	Pass
Tx.Origin Authentication	Pass	Pass
Signatures Replay	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass

StrategyCore.sol	
Re-entrancy	Pass
Access Management Hierarchy	Pass
Arithmetic Over/Under Flows	Pass
Unexpected Ether	Pass
Delegatecall	Pass
Default Public Visibility	Pass
Hidden Malicious Code	Pass
Entropy Illusion (Lack of Randomness)	Pass
External Contract Referencing	Pass
Short Address/Parameter Attack	Pass
Unchecked CALL Return Values	Pass
Race Conditions/Front Running	Pass
General Denial Of Service (DOS)	Pass
Uninitialized Storage Pointers	Pass
Floating Points and Precision	Pass
Tx.Origin Authentication	Pass
Signatures Replay	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass

CODE COVERAGE AND TEST RESULTS FOR ALL FILES

Tests written by Zokyo Security

As part of our work assisting IPOR in verifying the correctness of their contract code, our team was responsible for writing integration tests using the Truffle testing framework.

Tests were based on the functionality of the code, as well as a review of the IPOR contract requirements for details about issuance amounts and how the system handles these.

```
IpToken
  Deploy
    ✓ with wrong asset address (56ms)
  decimals
    ✓ decimals should be 18
  getAsset
    ✓ asset should be same with constructor param (56ms)
  setJoseph
    ✓ set with success
    ✓ wrong address
  mint
    ✓ mint with success
    ✓ wrong amount
    ✓ if caller not Joseph should revert
  burn
    ✓ burn with success
    ✓ wrong amount
    ✓ if caller not Joseph should revert
  tokens
    ✓ deploy IpTokenUsdt (764ms)
    ✓ deploy IpTokenUsdc (760ms)
    ✓ deploy IpTokenDai (755ms)
IporOracle
  initialize
    ✓ init with success (761ms)
    ✓ init multiple times
    ✓ wrong asset address (745ms)
  getVersion
    ✓ version should be 1
    ✓ version should greater than 0
  getIndex
```

✓ return with success
✓ asset not supported

getAccruedIndex

✓ return with success
✓ asset not supported

calculateAccruedIbtPrice

✓ return with success

updateIndex

✓ return with success
✓ call not from updater should revert

updateIndexses

✓ return with success
✓ diff length for assets and indexes
✓ update for unexisting asset should fail
✓ astUpdateTimestamp > updateTimestamp (803ms)

addUpdater

✓ add Updater with success
✓ call not from owner

removeUpdater

✓ remove Updater with success
✓ call not from owner

isUpdater

✓ updater exists
✓ updater not exists

addAsset

✓ add asset with success
✓ add an asset with wrong address should revert
✓ add an existing assets should revert

removeAsset

✓ remove asset with success
✓ remove an asset with wrong address should revert
✓ remove a non existing assets should return

pause

✓ set pause true
✓ set pause false

IporLogic

accrueQuasiIbtPrice

✓ accrueTimestamp < indexTimestamp should revert

calculateExponentialWeightedMovingVariance

✓ alpha too high should revert
✓ indexValue > exponentialMovingAverage
✓ spread cant be higher than 1

DecayFactorCalculation

calculate

- ✓ interval one
- ✓ interval two
- ✓ interval three

IvToken

Deploy

- ✓ with wrong asset address

decimals

- ✓ decimals should be 18

getAsset

- ✓ asset should be same with constructor param

setStanley

- ✓ set with success
- ✓ wrong address

mint

- ✓ mint with success
- ✓ wrong amount
- ✓ if caller not Joseph should revert

burn

- ✓ burn with success
- ✓ wrong amount
- ✓ if caller not Joseph should revert

tokens

- ✓ deploy IvTokenUsdt (760ms)
- ✓ deploy IvTokenUsdc (773ms)
- ✓ deploy IvTokenDai (744ms)

Stanley

- ✓ try initialize all fails (189ms)
- ✓ should check total balance (69ms)
- ✓ should check calculate exchange rate (92ms)
- ✓ should set milton (65ms)
- ✓ should check version
- ✓ should check asset (80ms)
- ✓ should deposit (123ms)
- ✓ should check pause/unpause (99ms)
- ✓ should withdraw, asset balance aave bigger then compound and amount is equal (216ms)
- ✓ should withdraw, asset balance aave lesseer then compound (180ms)
- ✓ should withdraw all, all chekcs (160ms)
- ✓ should migrate assets to strategy, all checks (207ms)
- ✓ should set strategy aave with already strategy in store slot (149ms)
- ✓ should set strategy compound with already strategy in store slot (192ms)

- ✓ should call authorize upgrade as not the owner
- ✓ should calculate exchange rate with total balance bigger then 0 iv token balance bigger then 0 (109ms)
- ✓ should withdraw from strategy with transfer set as false (134ms)

Core strategy

- ✓ should be able to use core strategy utilities (182ms)

Aave strategy

- ✓ should revert for zero input addresses (216ms)
- ✓ should get apr from reserve data (49ms)
- ✓ should get balance of sharetoken
- ✓ should set stkAave or revert for invalid address
- ✓ should execute beforeClaim or revert if treasury not set (38ms)
- ✓ should deposit to lending pool (94ms)
- ✓ should withdraw from lending pool (79ms)
- ✓ should execute doClaim (80ms)
- ✓ should revert claim if treasury not set

Compound strategy

- ✓ should revert deploy for zero addresses (124ms)
- ✓ should get apr
- ✓ should get balance of share token (40ms)
- ✓ should deposit asset (52ms)
- ✓ should withdraw asset (67ms)
- ✓ should execute doClaim or revert
- ✓ should execute doClaim or revert
- ✓ should set blocks per year or revert

Coverage test

- ✓ Should test coverage for IporOracleFacadeDataProvider (58ms)
- ✓ Should test coverage for CockpitDataProvider (492ms)
- ✓ Should test coverage for MiltonFacadeDataProvider (221ms)

Joseph

- ✓ Should be able to initialize properly (135ms)
- ✓ Should be able to initialize in a paused state (48ms)
- ✓ Should be able to check vault reserves ratio (92ms)
- ✓ Should be able to calculate exchange rate (72ms)
- ✓ Should be able to calculate Redeemed Utilization Rate
- ✓ Should be able to provide liquidity (94ms)
- ✓ Should be able to redeem (316ms)

JosephInternal

- ✓ Should be able to get version
- ✓ Should be able to set asset address
- ✓ Should set rebalance ratio (43ms)
- ✓ Should be able to get redeem fee rate

- ✓ Should be able to get Redeem Lp Max Utilization Rate
- ✓ Should be able to set treasury manager
- ✓ Should be able to get treasury manager
- ✓ Should be able to set charlie treasury manager
- ✓ Should be able to get charlie treasury manager
- ✓ Should be able to set charlie treasury
- ✓ Should be able to get charlie treasury
- ✓ Should be able to pause contract
- ✓ Should be able to unpause contract (40ms)
- ✓ Should be able to set treasury
- ✓ Should be able to get treasury
- ✓ Should deposit to stanley
- ✓ Should be able to transfer to treasury (209ms)
- ✓ Should be able to transfer to charlie treasury (113ms)
- ✓ Should be able to withdraw from stanley (41ms)
- ✓ Should be able to withdraw all from stanley (42ms)
- ✓ Should be able to rebalance (129ms)
- ✓ Should be able to set max lp account contribution
- ✓ Should be able to get max lp account contribution (41ms)
- ✓ Should be able to set max liquidity pool balance
- ✓ Should be able to get max lp account contribution (39ms)

Milton

- ✓ Should be initialized properly (125ms)
- ✓ Should be able to initialize contract in paused state (53ms)
- ✓ Should be able to calculate spread (112ms)
- ✓ Should be able to calculate soap (81ms)
- ✓ Should be able to calculate split opening fee amount (52ms)
- ✓ Should be able to open Swap Pay Fixed (379ms)
- ✓ Should be able to calculate Income Fee Value (54ms)
- ✓ Should be able to calculate swap indicators (74ms)
- ✓ Should be able to validate liquidity pool utylization
- ✓ Should be able to transfer tokens based on payoff (166ms)
- ✓ Should be able to close inactive swaps (98ms)
- ✓ Should be able to close swaps (190ms)
- ✓ Should be able to close swap pay fixed (195ms)
- ✓ Should be able to emergency Close fixed swap pay only when paused (189ms)
- ✓ Should be able to close fixed swap received (201ms)
- ✓ Should be able to emergency Close fixed swap received when contract is paused (164ms)
- ✓ Should be able to emergency Close fixed swaps received when contract is paused (236ms)
- ✓ Should be able to emergency Close swaps fixed pay received when contract is paused (232ms)
- ✓ Should be able to open swap receive fixed (389ms)

MiltonInternal

- ✓ Should be able to get version
- ✓ Should be able to get asset
- ✓ Should be able to get Ipor PublicationFee
- ✓ Should be able to get income Fee rate
- ✓ Should be able to get opening Fee rate
- ✓ Should be able to get Opening Fee Treasury Portion Rate
- ✓ Should be able to get max leverage
- ✓ Should be able to get min leverage
- ✓ Should be able to get liquidation deposit amount
- ✓ Should be able to get wad liquidation deposit amount
- ✓ Should be able to get max swap collateral amoun
- ✓ Should be able to get max LP utilization rate
- ✓ Should be able to get max LP utilization per leg rate
- ✓ Should be able to pause contract (46ms)
- ✓ Should be able to unpause contract (65ms)
- ✓ Should be able to set joseph (56ms)
- ✓ Should be able to get joseph (48ms)
- ✓ Should be able to set up max allowance for asset (96ms)
- ✓ Should be able to get milton spread model
- ✓ Should be able to set spread model (49ms)
- ✓ Should be able to get accrued balance (115ms)
- ✓ Should be able to deposit to stanley (111ms)
- ✓ Should be able to withdraw from stanley (76ms)
- ✓ Should be able to withdrawal from stanley (80ms)
- ✓ Should be able to get calculatePayoffPayFixed (53ms)
- ✓ Should be able to get calculatePayoffReceiveFixed (44ms)
- ✓ Should be able to get calculateSoapAtTimestamp (61ms)

MiltonStorage

- ✓ Should be initialized correctly
- ✓ Should be able to get version
- ✓ Should be able to set joseph (79ms)
- ✓ Should be able to add liquidity (181ms)
- ✓ Should be able to remove liquidity (119ms)
- ✓ Should be be able to get liquidity pool account contribution (79ms)
- ✓ Should be able to pause contract (45ms)
- ✓ Should be able to unpause contract (73ms)
- ✓ Should be able to set milton (57ms)
- ✓ Should be able to get extended balance
- ✓ Should be able to update storage when transfer to treasury (150ms)
- ✓ Should be able to update storage when transfer to charlie treasury (182ms)
- ✓ Should be able to update storage when deposit to stanley (176ms)
- ✓ Should be able to update storage when withdraw from stanley (169ms)

✓ Should be able to update storage when open swap pay fixed (113ms)
✓ Should be able to update storage when open swap receive fixed (95ms)
✓ Should be able to get last swap id (95ms)
✓ Should be able to get total outstanding notional (47ms)
✓ Should be able to get swap pay fixed (63ms)
✓ Should be able to get swap receive fixed (65ms)
✓ Should be able to calculate soap
✓ Should be able to get swaps fixed (70ms)
✓ Should be able to get swaps receive fixed (128ms)
✓ Should be able to get swap pay fixed ids (117ms)
✓ Should be able to get swaps receive fixed (114ms)
✓ Should be able to calculate soap
✓ Should be able to calculate soap pay fixed
✓ Should be able to update balance when close swap (108ms)
✓ Should be able to update storage when close swap pay fixed (397ms)
✓ Should be able to update storage when close swap receive fixed (468ms)
✓ Should be able to get Swap Ids (145ms)

212 passing (3m)

FILE	% STMTS	% BRANCH	% FUNCS	% LINES	% Uncovered Lines
Milton	100	91.89	97.06	100	
MiltonInternal	100	100	100	100	
MiltonStorage	99.55	97.06	98.04	99.56	236
MiltonUsdc	100	100	100	100	
Joseph	100	93.75	100	100	
JosephInternal	97.83	97.5	97.3	97.67	152,156
IporOracle	100	100	100	100	
IpToken	100	100	100	100	
IvToken	100	100	100	100	
Stanley	100	100	100	95.65	
StanleyDai	100	100	100	100	
StrategyAave	100	96.43	100	100	

StrategyCompound	100	100	100	100
StrategyCore	100	100	92.86	100
All files	**99.68**	**96.88**	**97.81**	**99.68**

We are grateful to have been given the opportunity to work with the IPOR team.

The statements made in this document should not be interpreted as an investment or legal advice, nor should its authors be held accountable for the decisions made based on them.

Zokyo's Security Team recommends that the IPOR team put in place a bug bounty program to encourage further analysis of the smart contract by third parties.

ZOKYO.