SAFUAUDIT
SMART CONTRACT AUDITING

PONZI PROTOCOL

SMART CONTRACT AUDIT

April 3, 2022

INTRODUCTION

Client	Ponzi Protocol (PPCoin)
Language	Solidity
Contract address	0xE1dA654cE29AF88490b2e2a66D54cc4F54392031
Decimals	5
Supply	100,000
Platform	Binance Smart Chain
Compiler	v0.8.13+commit.abaa5c0e
Optimization	Yes, with 200 runs
Website	https://ponzi-protocol.com/
Discord	https://discord.com/invite/2zYbGRhEHn
Twitter	https://twitter.com/Ponzi_Protocol

Description

Ponzi Protocol is a next-generation auto-staking project that rewards its' holders with incredibly high variable APY and rewards in $BUSD while retaining a fair taxation percentage. Ponzi Protocol has a high burn and auto-liquidity engine built-in, and many other improvements over other similar tokens.

TABLE OF CONTENTS

Approach

Audit Details

Our comprehensive audit report provides a full overview of the audited system's architecture, smart contract codebase, and details on any vulnerabilities found within the system.

Audit Goals

The audit goal is to ensure that the project is built to protect investors and users, preventing potentially catastrophic vulnerabilities after launch, that lead to scams and rugpulls.

Code Quality

Our analysis includes both automatic tests and manual code analysis for the following aspects:

- Exploits
- Back-doors
- Vulnerability
- Accuracy
- Readability

Tools

- Remix IDE
- MythX, Mythril
- SWC Registry
- Open Zeppelin Code Analyzer
- Solidity Code Complier

RISK CLASSIFICATION

CRITICAL

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

MEDIUM

Issues on this level could potentially bring problems and should eventually be fixed.

MINOR

Issues on this level are minor details and warning that can remain unfixed but would be better fixed at some point in the future

INFORMATIONAL

Information level is to offer suggestions for improvement of efficacity or security for features with a risk free factor.

ABSTRACT

Fees	Ownership	Mint function
Buy Fees: 10% Sell Fees: 15%	Owned	Rebase Token

Owner can set fees	Max Tx amount	Pause
Owner can set fees up to 20%	Owner can't set max Tx amount	Owner can't pause trading

Vulnerabilities Test

SWC ID	Description	
SWC-100	Function Default Visibility	Passed
SWC-101	Integer Overflow and Underflow	Passed
SWC-102	Outdated Compiler Version	Passed
SWC-103	Floating Pragma	Minor
SWC-104	Unchecked Call Return Value	Medium
SWC-105	Unprotected Ether Withdrawal	Passed
SWC-106	Unprotected SELF-DESTRUCT Instruction	Passed
SWC-107	Re-entrancy	Passed
SWC-108	State Variable Default Visibility	Minor
SWC-109	Uninitialized Storage Pointer	Passed
SWC-110	Assert Violation	Passed
SWC-111	Use of Deprecated Solidity Functions	Passed
SWC-112	Delegate Call to Untrusted Callee	Passed
SWC-113	DoS with Failed Call	Passed
SWC-114	Transaction Order Dependence	Passed
SWC-115	Authorization through tx.origin	Minor

SWC-116	Block values as a proxy for time	**Passed**
SWC-117	Signature Malleability	**Passed**
SWC-118	Incorrect Constructor Name	**Passed**
SWC-119	Shadowing State Variables	**Passed**
SWC-120	Weak Sources of Randomness from Chain Attributes	**Minor**
SWC-121	Missing Protection against Signature Replay Attacks	**Passed**
SWC-122	Lack of Proper Signature Verification	**Passed**
SWC-123	Requirement Violation	**Passed**
SWC-124	Write to Arbitrary Storage Location	**Passed**
SWC-125	Incorrect Inheritance Order	**Passed**
SWC-126	Insufficient Gas Griefing	**Passed**
SWC-127	Arbitrary Jump with Function Type Variable	**Passed**
SWC-128	DoS With Block Gas Limit	**Passed**
SWC-129	Typographical Error	**Passed**
SWC-130	Right-To-Left-Override control character (U+202E)	**Passed**
SWC-131	Presence of unused variables	**Passed**
SWC-132	Unexpected Ether balance	**Passed**
SWC-133	Hash Collisions With Multiple Variable Length Arguments	**Passed**
SWC-134	Message call with the hardcoded gas amount	**Passed**
SWC-135	Code With No Effects (Irrelevant/Dead Code)	**Passed**
SWC-136	Unencrypted Private Data On-Chain	**Passed**

MANUAL ANALYSIS

The contract is verified to check if functions do and work as they should and malicious code is not inserted.

	Tested	Result
Transfer	Yes	**Passed**
Total Supply	Yes	**Passed**
Buy Back	Yes	**N/A**
Burn	Yes	**N/A**
Mint	Yes	**N/A**
Rebase	Yes	**Medium**
Pause	Yes	**N/A**
Blacklist	Yes	**Passed**
Lock	Yes	**N/A**
Max Transaction	Yes	**N/A**
Transfer Ownership	Yes	**Passed**
Renounce Ownership	Yes	**Passed**

CONTRACT INSPECTION

Owners	Implementation			
└	<Constructor>	Public ❗	🛑	NO❗
└	isOwner	Public ❗		NO❗
└	getOwners	External ❗		NO❗
└	addOwner	Public ❗	🛑	onlyMasterOwner
└	removeOwner	Public ❗	🛑	onlyMasterOwner
└	renounceOwnership	External ❗	🛑	onlyMasterOwner
PauseOwners	Implementation	Owners		
└	pauseGuard	Internal 🔒		
└	modifyPauseExempt	External ❗	🛑	onlyOwners
IERC20	Interface			
└	totalSupply	External ❗		NO❗
└	balanceOf	External ❗		NO❗
└	allowance	External ❗		NO❗
└	transfer	External ❗	🛑	NO❗
└	approve	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
IPancakeSwapPair	Interface			
└	name	External ❗		NO❗
└	symbol	External ❗		NO❗
└	decimals	External ❗		NO❗
└	totalSupply	External ❗		NO❗
└	balanceOf	External ❗		NO❗
└	allowance	External ❗		NO❗
└	approve	External ❗	🛑	NO❗
└	transfer	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
└	DOMAIN_SEPARATOR	External ❗		NO❗
└	PERMIT_TYPEHASH	External ❗		NO❗
└	nonces	External ❗		NO❗
└	permit	External ❗	🛑	NO❗

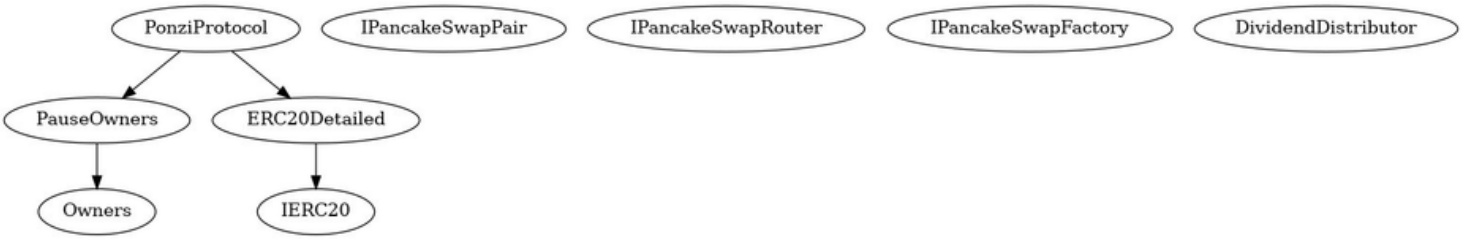
└	MINIMUM_LIQUIDITY	External ❗			NO❗
└	factory	External ❗			NO❗
└	token0	External ❗			NO❗
└	token1	External ❗			NO❗
└	getReserves	External ❗			NO❗
└	price0CumulativeLast	External ❗			NO❗
└	price1CumulativeLast	External ❗			NO❗
└	kLast	External ❗			NO❗
└	mint	External ❗	🛑		NO❗
└	burn	External ❗	🛑		NO❗
└	swap	External ❗	🛑		NO❗
└	skim	External ❗	🛑		NO❗
└	sync	External ❗	🛑		NO❗
└	initialize	External ❗	🛑		NO❗
IPancakeSwapRouter	Interface				
└	factory	External ❗			NO❗
└	WETH	External ❗			NO❗
└	addLiquidity	External ❗	🛑		NO❗
└	addLiquidityETH	External ❗	💵		NO❗
└	removeLiquidity	External ❗	🛑		NO❗
└	removeLiquidityETH	External ❗	🛑		NO❗
└	removeLiquidityWithPermit	External ❗	🛑		NO❗
└	removeLiquidityETHWithPermit	External ❗	🛑		NO❗
└	swapExactTokensForTokens	External ❗	🛑		NO❗
└	swapTokensForExactTokens	External ❗	🛑		NO❗
└	swapExactETHForTokens	External ❗	💵		NO❗
└	swapTokensForExactETH	External ❗	🛑		NO❗
└	swapExactTokensForETH	External ❗	🛑		NO❗
└	swapETHForExactTokens	External ❗	💵		NO❗
└	quote	External ❗			NO❗
└	getAmountOut	External ❗			NO❗
└	getAmountIn	External ❗			NO❗
└	getAmountsOut	External ❗			NO❗
└	getAmountsIn	External ❗			NO❗
└	removeLiquidityETHSupportingFeeOnTransferTokens	External ❗	🛑		NO❗
└	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External ❗	🛑		NO❗
└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	🛑		NO❗
└	swapExactETHForTokensSupportingFeeOnTransferTokens	External ❗	💵		NO❗
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑		NO❗

IPancakeSwapFactory	Interface			
└	feeTo	External ❗		NO❗
└	feeToSetter	External ❗		NO❗
└	getPair	External ❗		NO❗
└	allPairs	External ❗		NO❗
└	allPairsLength	External ❗		NO❗
└	createPair	External ❗	🛑	NO❗
└	setFeeTo	External ❗	🛑	NO❗
└	setFeeToSetter	External ❗	🛑	NO❗
DividendDistributor	Implementation			
└	<Constructor>	Public ❗	🛑	NO❗
└	setDistributionCriteria	External ❗	🛑	onlyToken
└	setShare	External ❗	🛑	onlyToken
└	deposit	External ❗	💵	onlyToken
└	process	External ❗	🛑	onlyToken
└	shouldDistribute	Internal 🔒		
└	distributeDividend	Internal 🔒	🛑	
└	claimDividend	Public ❗	🛑	NO❗
└	getUnpaidEarnings	Public ❗		NO❗
└	getShareholder	External ❗		NO❗
└	getCumulativeDividends	Internal 🔒		
└	addShareholder	Internal 🔒	🛑	
└	removeShareholder	Internal 🔒	🛑	
ERC20Detailed	Implementation	IERC20		
└	<Constructor>	Public ❗	🛑	NO❗
└	name	Public ❗		NO❗
└	symbol	Public ❗		NO❗
└	decimals	Public ❗		NO❗
PonziProtocol	Implementation	ERC20Detailed, PauseOwners		
└	<Constructor>	Public ❗	🛑	ERC20Detailed
└	activateTrade	External ❗	🛑	onlyOwners
└	antibotGuard	Private 🔐	🛑	
└	rebase	Internal 🔒	🛑	
└	transfer	External ❗	🛑	validRecipient
└	transferFrom	External ❗	🛑	validRecipient
└	_basicTransfer	Internal 🔒	🛑	
└	_transferFrom	Internal 🔒	🛑	

└	takeFee	Internal 🔒	🛑	
└	addLiquidity	Internal 🔒	🛑	swapping
└	swapBack	Internal 🔒	🛑	swapping
└	manualWithdraw	External ❗	🛑	swapping onlyOwners
└	swapToETH	Private 🔐	🛑	
└	shouldTakeFee	Internal 🔒		
└	shouldRebase	Internal 🔒		
└	shouldAddLiquidity	Internal 🔒		
└	shouldSwapBack	Internal 🔒		
└	setRebaseSettings	External ❗	🛑	onlyOwners
└	setRebaseHalvingSettings	External ❗	🛑	onlyOwners
└	setAutoAddLiquiditySettings	External ❗	🛑	onlyOwners
└	allowance	External ❗		NO❗
└	approve	External ❗	🛑	NO❗
└	setIsDividendExempt	External ❗	🛑	onlyOwners
└	setDividendDistributionCriteria	External ❗	🛑	onlyOwners
└	setDividendDistributorGas	External ❗	🛑	onlyOwners
└	getCirculatingSupply	Public ❗		NO❗
└	getCirculatingSupplyExcludingLiquidity	Public ❗		NO❗
└	isNotInSwap	External ❗		NO❗
└	manualSync	External ❗	🛑	NO❗
└	setFeeReceivers	External ❗	🛑	onlyOwners
└	checkFeeExempt	External ❗		NO❗
└	setFeeExempt	External ❗	🛑	onlyOwners
└	setBuyFees	External ❗	🛑	onlyOwners
└	setSellFees	External ❗	🛑	onlyOwners
└	getLiquidityBacking	Public ❗		NO❗
└	setBotBlacklist	External ❗	🛑	onlyOwners
└	totalSupply	External ❗		NO❗
└	balanceOf	Public ❗		NO❗
└	isContract	Internal 🔒		
└	<Receive Ether>	External ❗	💵	NO❗

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable
🔐	Private function
🔒	Internal function
NO❗	Function has no modifier

INHERITANCE TREE



Inheritance is a feature of the object-oriented programming language. It is a way of extending the functionality of a program, used to separate the code, reduces the dependency, and increases the re-usability of the existing code. Solidity supports inheritance between smart contracts, where multiple contracts can be inherited into a single contract.

Important Snippets

Owner can set buy and sell fees but only to a limit of 20%

```
function setBuyFees(uint256 _liquidityFee,uint256 _dividendFee,uint256 _treasuryFee) external onlyOwners {
    require(_liquidityFee + _dividendFee + _treasuryFee <= maxTotalFee);
    buyLiquidityFee = _liquidityFee;
    buyDividendFee = _dividendFee;
    buyTreasuryFee = _treasuryFee;
}

function setSellFees(uint256 _burnFee, uint256 _liquidityFee,uint256 _dividendFee,uint256 _treasuryFee) external onlyOwners {
    require(_burnFee + _liquidityFee + _dividendFee + _treasuryFee <= maxTotalFee);
    sellBurnFee = _burnFee;
    sellLiquidityFee = _liquidityFee;
    sellDividendFee = _dividendFee;
    sellTreasuryFee = _treasuryFee;
}
```

Blacklisted addresses are not permitted to transfer their tokens

```
function setBotBlacklist(address _address, bool _flag) external onlyOwners {
    if (isContract(_address) && _address != pair) {
        botBlacklist[_address] = _flag;
    } else {
        require(
            !_flag,
            "Can only disable blacklist for user owner addresses"
        );
        botBlacklist[_address] = _flag;
    }
}
```

Owners can change rebase settings without a set limit

```
function setRebaseSettings(bool enabled,uint256 interval,uint256 rate) external onlyOwners {
    _autoRebase = enabled;
    rebaseInterval = interval;
    rebaseRate = rate;
    _lastRebasedTime = block.timestamp;
}

function setRebaseHalvingSettings(bool enabled, uint256 interval) external onlyOwners {
    rebaseRateHalvingEnabled = enabled;
    rebaseRateHalvingInterval = interval;
    _lastRebasedTime = block.timestamp;
}
```

GOOD PRACTICES

- The owner cannot stop or pause the smart contract
- The owner cannot set max Tx
- The owner cannot set fees more than 20%

WEBSITE

Website	https://ponzi-protocol.com/
Domain Registry	http://www.namecheap.com
Domain Expiry Date	2023-03-30
Response Code	200
SSL Checker and HTTPS Test	Passed
Deprecated HTML tags	Passed
Robots.txt	Passed
Sitemap Test	Informational
SEO Friendly URL	Passed
Responsive Test	Passed
JS Error Test	Passed
Console Errors Test	Passed
Site Loading Speed Test	1.93 seconds - Passed
HTTP2 Test	Informational
Safe Browsing Test	Passed

DISCLAIMER

SafuAudit.com is not a financial institution and the information provided on this website does not constitute investment advice, financial advice, trading advice or any other sort of advice. You should not treat any of the website's content as such. Investing in crypto assets carries a high level of risk and does not hold guarantees for not sustaining financial loss due to their volatility.

Accuracy of Information

SafuAudit will strive to ensure accuracy of information listed on this website although it will not hold any responsibility for any missing or wrong information. SafuAudit provides all information as is. You understand that you are using any and all information available here at your own risk. Any use or reliance on our content and services is solely at your own risk and discretion.

The purpose of the audit is to analyse the on-chain smart contract source code, and to provide basic overview of the project.

While we have used all the information available to us for this straightforward investigation, you should not rely on this report only — we recommend proceeding with several independent audits Be aware that smart contracts deployed on a blockchain aren't secured enough against external vulnerability, or a hack. Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security. Therefore, SafuAudit does not guarantee the explicit security of the audited smart contract. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

AUDIT RESULTS

CRITICAL

No critical severity issues have been found.

MEDIUM

- Rebase settings functions (setRebaseSettings, setRebaseHalvingSettings, setAutoAddLiquiditySettings) can be adjusted by owners without a set limit.
- Unchecked return value from low-level external call. Low-level external calls return a boolean value. If the callee halts with an exception, 'false' is returned and execution continues in the caller. The caller should check whether an exception happened and react accordingly to avoid unexpected behavior. Line 1133 and line 1150

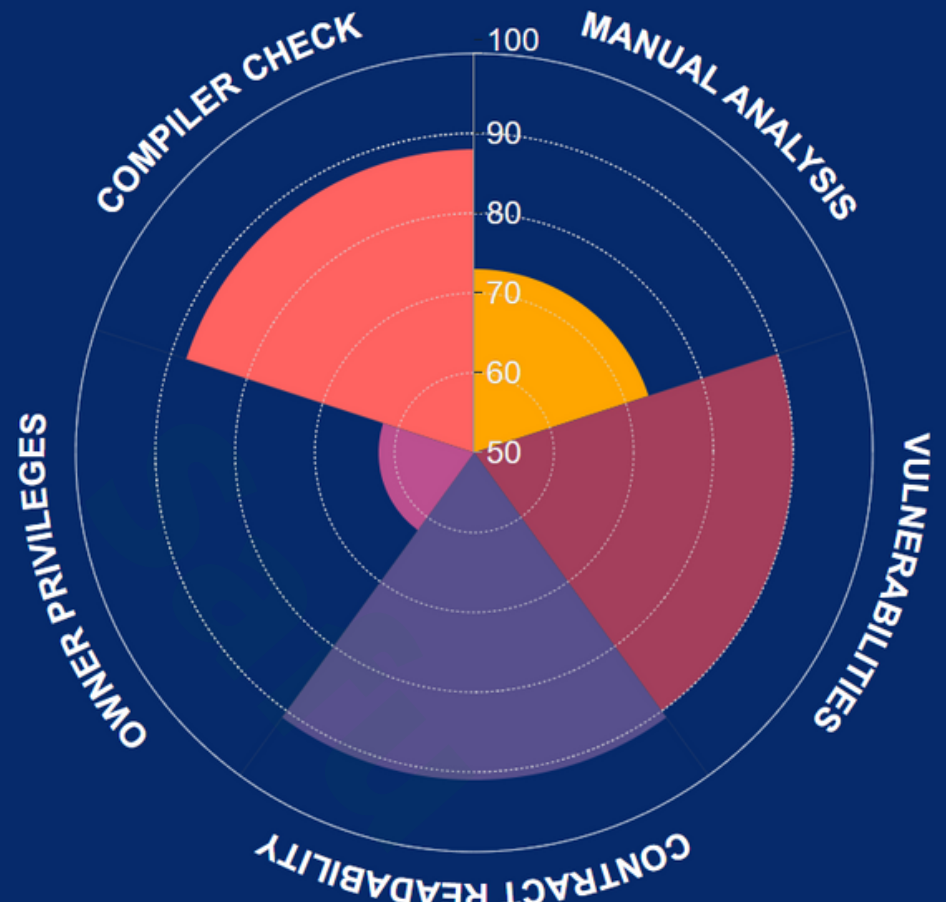
MINOR

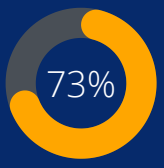
- A floating pragma is set. It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.
- State variable visibility is not set for: _token, rewardToken, router, shareholders, shareholderIndexes, shareholderClaims, initialized, inSwap
- Potential use of "block.number" as source of randonmness. The environment variable "block.number" looks like it might be used as a source of randomness. Note that the values of variables like coinbase, gaslimit, block number and timestamp are predictable
- Using "tx.origin" as a security control can lead to authorization bypass vulnerabilities. Consider using "msg.sender" instead.

INFORMATIONAL

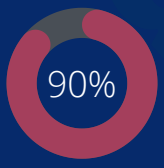
No informational data or suggestions for risk free features have been found

SAFUSCORE

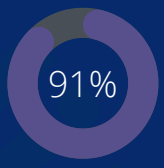




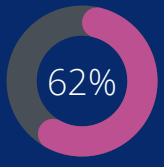
Manual Analysis



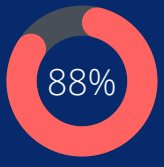
Vulnerabilities



Contract Readability



Owner Privileges

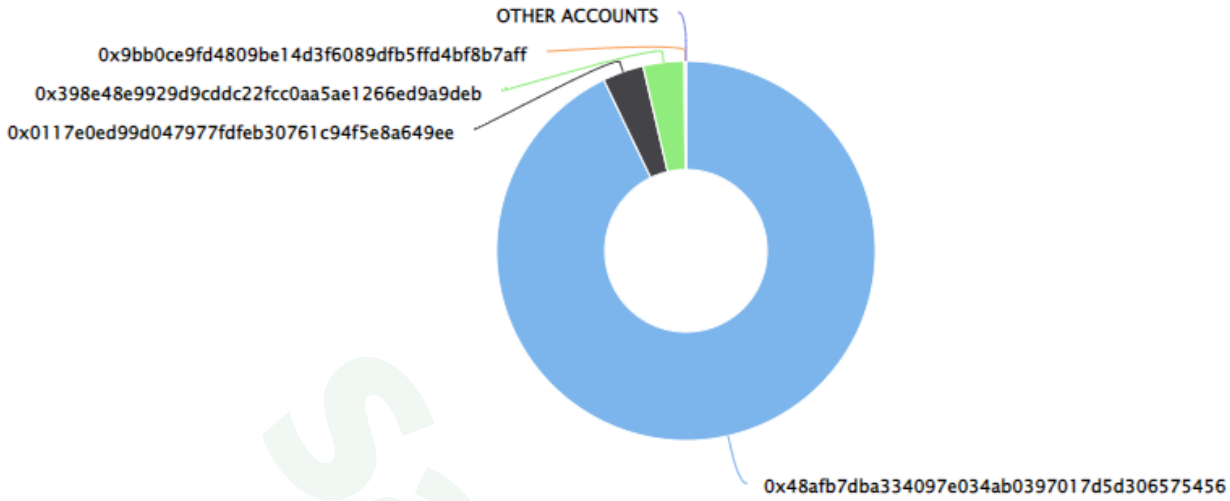


Compiler Check

Final Score:80.8

SUMMARY

Top 10 holders



Rank	Address	Quantity (Token)	Percentage
1	0x48afb7dba334097e034ab0397017d5d306575456	92,868	92.8680%
2	0x0117e0ed99d047977fdfeb30761c94f5e8a649ee	3,500	3.5000%
3	0x398e48e9929d9cddc22fcc0aa5ae1266ed9a9deb	3,500	3.5000%
4	0x9bb0ce9fd4809be14d3f6089dfb5ffd4bf8b7aff	132	0.1320%

Conclusion

Project Ponzi Protocol (PPCoin) does not contain any severe issues. It utilizes rebase function that increases or decreases total supply and can be adjusted according to some parameters that have arbitrary limits set.

SafuAudit has tested the security based on manual and automated tests. Please note that we don't offer any warranties for business model.

SafuAudit.com