



Cyberscope

Audit Report

BeraTrax

March 2025

Files Vault, ArberaZapper, InfraredZapper, KodiakZapper, SteerZapper, ZapperBase, LpRouter, SwapRouter, ArberaStrategy, InfraredStrategy, KodiakStrategy, SteerStrategy, SInfraredFactory, StrategyBase, ArberaFactory, KodiakFactory, SteerFactory, StrategyFactoryBase, VaultFactory, ControllerFactory, Controller

Audited by © cyberscope

Table of Contents

Table of Contents	1
Risk Classification	4
Review	5
Audit Updates	5
Source Files	5
Overview	7
Controller	7
Factories	7
Strategies	7
Vault	8
Zappers	8
Disclaimer	8
Findings Breakdown	9
Diagnostics	10
EPTTNA - Exit Pool Token Transfer Not Assured	12
Description	12
Recommendation	13
IFAC - Incorrect Fee Amount Calculation	14
Description	14
Recommendation	14
QEF - Quote Excludes Fees	15
Description	15
Recommendation	17
ILU - Inconsistent Library Use	18
Description	18
Recommendation	18
CR - Code Repetition	19
Description	19
Recommendation	20
CCR - Contract Centralization Risk	21
Description	21
Recommendation	23
ELFM - Exceeds Fees Limit	24
Description	24
Recommendation	25
GRLNS - Gamma Remove Liquidity Not Supported	26
Description	26
Recommendation	26
MC - Missing Check	27

Description	27
Recommendation	27
MN - Misspelled Naming	28
Description	28
Recommendation	29
ORA - Overwriting Rewards Amount	30
Description	30
Recommendation	30
PZAZI - Possible Zero Amount Zap In	31
Description	31
Recommendation	31
PLPI - Potential Liquidity Provision Inadequacy	32
Description	32
Recommendation	34
SAU - Swapped Amount Uninitialized	35
Description	35
Recommendation	35
USV - Uninitialized State Variable	36
Description	36
Recommendation	36
UBUFL - Unintended Balance Used For Liquidity	37
Description	37
Recommendation	38
UTPD - Unverified Third Party Dependencies	39
Description	39
Recommendation	40
L02 - State Variables could be Declared Constant	41
Description	41
Recommendation	41
L04 - Conformance to Solidity Naming Conventions	42
Description	42
Recommendation	42
L09 - Dead Code Elimination	43
Description	43
Recommendation	43
L14 - Uninitialized Variables in Local Scope	44
Description	44
Recommendation	44
L15 - Local Scope Variable Shadowing	45
Description	45
Recommendation	45
L17 - Usage of Solidity Assembly	46

Description	46
Recommendation	46
Functions Analysis	47
Inheritance Graph	63
Summary	64
Disclaimer	65
About Cyberscope	66

Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation:** This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation:** This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical:** Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium:** Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor:** Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative:** Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
● Critical	Highly Likely / High Impact
● Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
● Minor / Informative	Unlikely / Low to no Impact

Review

Audit Updates

Initial Audit	17 Jan 2025 https://github.com/cyberscope-io/audits/blob/main/c5-btx/v1/audit.pdf
Corrected Phase 2	31 Jan 2025 https://github.com/cyberscope-io/audits/blob/main/c5-btx/v2/audit.pdf
Corrected Phase 3	09 Mar 2025

Source Files

Filename	SHA256
controllers/Controller.sol	d1dbd00e30ebfc4ce21b48d43c5799d6593c2b70a878358068e759a9d468616b
factories/ArberaFactory.sol	37320f3de510b1e8726a1fcb22f23145e33779ee48618dd8df1997bc3532bfff
factories/ControllerFactory.sol	eed63c88d2896f9f85db51e50df0024b3890fd74fb834d141c03852321d48cfc
factories/InfraredFactory.sol	86b2418582f27a17e22cf117b3b252becc9c8464a57b2ba20cc816941faafaac
factories/KodiakFactory.sol	a745d58121f1d2ec887ba7460f33ac078ae1713cf11794c6b9ebb761a5aa2531
factories/SteerFactory.sol	6aac96481f34974bf86849962d3c10fa201ac66b7f7ff9effb571ee5bd9e76ca
factories/StrategyFactoryBase.sol	4c293174ad20551ba5d31c1273c818d61d725c135ffab9e3e26641e786d6329c
factories/VaultFactory.sol	e9230c9b34c80543b9eaa2e6906d90fa43bfa12346775f8b1c8c1a5fd0ff32c4
strategies/ArberaStrategy.sol	d780c7c63a8ea516fe926bc765fe321e9db4dc6a01c77d4875769178b965ef56

strategies/InfraredStrategy.sol	3de78e266f673d385fca220f6cd6d9f1c28407a80ea8605d009b46370fe89402
strategies/KodiakStrategy.sol	289809d4c4937f7d0573528ad5f38ae89b3e440680c95ca69985e61ce938b234
strategies/SteerStrategy.sol	3ad54d64918c52ca51d99927de12d2aea0fa7bf7d78758fc35117622e6a31c99
strategies/StrategyBase.sol	9b60c9f9823592ebf21dfec4cc4cc35cbde3acd28189d68d34d41c607bfb653a
utils/LpRouter.sol	34d9b150009f5c024a08c58821ebb0b09484234bc83942eabc90883ebab418b5
utils/SwapRouter.sol	9e9bc3e56b04e1252db0102ed053f85a39ae621ccddc3f63741ef7eabae4094b
vaults/Vault.sol	478b5199f40ccf76f53b869c12c372611422fa398f67743fd339b4b0d07db672
zappers/ArberaZapper.sol	206996b2132ba507f78a279a8be2d6a6546567057b15f58393bc54ef206b928f
zappers/InfraredZapper.sol	91589b8443c8796938c9bb3f573513462ffacce7847532b57365029768ecff9
zappers/KodiakZapper.sol	c1ea8b88071979dc5e86e10a370661daaa4c893f0332c8094a065c4e1536d4a8
zappers/SteerZapper.sol	14c39cbfb5d8ad41464833fae547df7f005f91ac59840a345fc4404da347b25c
zappers/ZapperBase.sol	b7d5e55b542d1fa69ad576ebbb884a196d6487bbd67071c4013bb6fe1bfa208b

Overview

The contracts implement a modular and efficient yield aggregator built on the Ethereum Virtual Machine (EVM). Contrax optimises yield generation by utilising a combination of smart contracts that automate asset management and maximise returns. The dApp provides users with a seamless platform to deposit their assets and earn competitive APR. Its architecture is designed for scalability, security, and flexibility, ensuring that users can confidently participate in an efficient and transparent ecosystem for yield farming.

Controller

The Controller serves as the central management layer connecting the Vaults to their respective investment Strategies. Its primary purpose is to oversee the flow of funds from the Vaults to the Strategies and ensure that assets are optimally allocated to generate yield. The Controller maintains control over approved Strategies, allowing governance to update or revoke them as needed to adapt to changing market conditions. By acting as an intermediary, the Controller provides a secure and modular architecture, separating user deposits from the underlying investment logic while enforcing robust access controls and operational flexibility.

Factories

The Factory is responsible for the deployment and initialization of Vaults and Controllers, enabling a seamless creation process for these core components. By standardizing the deployment of Vault-Controller pairs, the Factory ensures consistency in configuration and governance integration. It allows for scalability and adaptability by enabling developers and strategists to deploy new Vaults and Controllers for different assets, while ensuring the system adheres to predefined rules and relationships. As a central hub for new deployments, the Factory streamlines the expansion of the protocol while maintaining security and governance integrity.

Strategies

The Strategies are the yield-generating engines of the system, implementing specific logic for investing assets into staking pools, liquidity farms, or other financial products. Their goal is to maximize returns on assets deposited by the Vaults while adhering to risk and

operational constraints defined by governance. Each Strategy is tailored to a specific investment opportunity and can be updated or replaced as market conditions evolve. By abstracting investment logic, Strategies provide flexibility and modularity, allowing the protocol to adapt quickly to new yield sources without impacting the user-facing components of the system.

Vault

The Vault is the user-facing contract that manages deposits, withdrawals, and the representation of user stakes through Vault shares. When users deposit assets into the Vault, they receive shares that represent their proportional claim to the total assets under management. The Vault works closely with the Controller to allocate idle assets to Strategies through the `earn` function, ensuring that deposits are continuously put to productive use. During withdrawals, the Vault redeems shares for assets, either using its own reserves or retrieving funds from the Controller. By acting as a secure intermediary, the Vault simplifies user interactions while managing the complexities of yield generation.

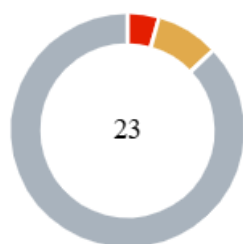
Zappers

The Zappers are designed to enhance user convenience by automating asset conversions and liquidity provision for deposits and withdrawals. They allow users to interact with Vaults using various tokens, handling the necessary swaps, liquidity additions, and token approvals behind the scenes. Zappers streamline the process of entering and exiting Vaults, eliminating the need for users to manually manage token conversions or intermediate steps. By abstracting away these complexities, Zappers improve accessibility and usability, enabling a broader range of users to participate in the protocol's yield-generating ecosystem.

Disclaimer

@spherex-xyz/contracts, being an external source, are considered out of scope for this review and will not be analyzed as part of this assessment.

Findings Breakdown



Critical	1
Medium	2
Minor / Informative	20

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	1	0	0	0
Medium	2	0	0	0
Minor / Informative	20	0	0	0

Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	EPTTNA	Exit Pool Token Transfer Not Assured	Unresolved
●	IFAC	Incorrect Fee Amount Calculation	Unresolved
●	QEF	Quote Excludes Fees	Unresolved
●	ILU	Inconsistent Library Use	Unresolved
●	CR	Code Repetition	Unresolved
●	CCR	Contract Centralization Risk	Unresolved
●	ELFM	Exceeds Fees Limit	Unresolved
●	GRLNS	Gamma Remove Liquidity Not Supported	Unresolved
●	MC	Missing Check	Unresolved
●	MN	Misspelled Naming	Unresolved
●	ORA	Overwriting Rewards Amount	Unresolved
●	PZAZI	Possible Zero Amount Zap In	Unresolved
●	PLPI	Potential Liquidity Provision Inadequacy	Unresolved

●	SAU	Swapped Amount Uninitialized	Unresolved
●	USV	Uninitialized State Variable	Unresolved
●	UBUFL	Unintended Balance Used For Liquidity	Unresolved
●	UTPD	Unverified Third Party Dependencies	Unresolved
●	L02	State Variables could be Declared Constant	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L09	Dead Code Elimination	Unresolved
●	L14	Uninitialized Variables in Local Scope	Unresolved
●	L15	Local Scope Variable Shadowing	Unresolved
●	L17	Usage of Solidity Assembly	Unresolved

EPTTNA - Exit Pool Token Transfer Not Assured

Criticality	Critical
Location	LpRouter.sol#L649,673
Status	Unresolved

Description

`_removeLiquidityBex` uses `_handleRemainingTokens` to send the tokens received from the `exitPool` to the user. However, in the message the `exitTokenIndex` is equal to `tokens.length - 2`. Any intermediate token received cannot be handled by `_handleRemainingTokens` since it only handles `token[0]` and `[tokens.length - 1]`.

```

function _prepareExitPoolRequest(
    IERC20[] memory tokens,
    uint256 lpAmount
) internal pure returns (IBeraVault.ExitPoolRequest memory request) {
    //...
    request.userData = tokens.length == 2
        ?
    abi.encode(WeightedPoolUserData.ExitKind.EXACT_BPT_IN_FOR_TOKEN
    S_OUT, lpAmount)
        : abi.encode(
    StablePoolUserData.ExitKind.EXACT_BPT_IN_FOR_ONE_TOKEN_OUT,
        lpAmount,
        tokens.length - 2
    );
    //...
}

function _removeLiquidityBex(
    IBeraPool lp,
    uint256 lpAmount,
    address recipient,
    address tokenOut
) internal sphereXGuardInternal(0x4f207669) returns (uint256 tokenOutAmount) {
    //...
    (IERC20[] memory tokens, , ) =
    IBeraVault(beraVault).getPoolTokens(poolId);
    //...
    tokenOutAmount = _handleRemainingTokens(
        tokenOut,
        address(tokens[0]),
        address(tokens[tokens.length - 1]),
        recipient
    );
}

```

Recommendation

It is recommended to make the adjustments necessary to ensure that users will receive their tokens after they remove liquidity. This can be achieved by specifying a specific token index to be received.

IFAC - Incorrect Fee Amount Calculation

Criticality	Medium
Location	ArberaZapper.sol#L562,565
Status	Unresolved

Description

`zapOutWithBond` checks if the `vault.asset()` is the `tokenOut`. If it is not it makes the swap to get the appropriate token. However the fees from `_transferFee` are calculated based on the `assetsOut` and not on the `tokenOutAmount` out.

```
if (vault.asset() == tokenOut) {
    tokenOutAmount = assetsOut;
} else {
    (tokenOutAmount, returnedAssets) =
    swapFromAssetsWithBond(vault.asset(), tokenOut, assetsOut,
    address(this));
}
(assetsOut, feeAmount) = _transferFee(tokenOut, zapOutFee,
assetsOut);
```

Recommendation

It is recommended to calculate the fees based on the `tokenOutAmount` or before making the swap.

QEF - Quote Excludes Fees

Criticality	Medium
Location	SwapRouter.sol#L696,739
Status	Unresolved

Description

The function `_getQuoteV3WithPath` is called by `_getQuoteV3` when `poolAddress` is `address(0)`. Both do not account for the fee percentage of the decentralize exchange when calculating the `amountOut`. In case of `_getQuoteV3WithPath` this leads to an overestimation of `amountOut` in multi-hop swaps, as each intermediate swap incurs a fee that is not deducted. This results in possible inaccurate quotes.


```
function _getQuoteV3(
    address tokenIn,
    address tokenOut,
    uint256 amountIn,
    address factory,
    bool isFeeProtocolTypeUint32
) internal view returns (uint256 amountOut) {
    (address poolAddress, ) = _findMostLiquidV3Pool(tokenIn,
tokenOut, factory);
    if (poolAddress == address(0)) {
        address[] memory path = new address[](3);
        path[0] = tokenIn;
        path[1] = wrappedNative;
        path[2] = tokenOut;
        return _getQuoteV3WithPath(path, amountIn, factory,
isFeeProtocolTypeUint32);
    }
    //...
}

function _getQuoteV3WithPath(
    address[] memory path,
    uint256 amountIn,
    address factory,
    bool isFeeProtocolTypeUint32
) internal view returns (uint256 amountOut) {
    for (uint256 i = 0; i < path.length - 1; i++) {
        (address poolAddress, ) =
_findMostLiquidV3Pool(path[i], path[i + 1], factory);
        if (poolAddress == address(0)) revert
NoPoolFoundForMultihopQuote();
        int24 tick;
        if (isFeeProtocolTypeUint32) {
            IUniswapV3PoolWithUint32FeeProtocol pool =
IUniswapV3PoolWithUint32FeeProtocol(poolAddress);
            (, tick, , , , ) = pool.slot0();
        } else {
            IUniswapV3Pool pool = IUniswapV3Pool(poolAddress);
            (, tick, , , , ) = pool.slot0();
        }
        amountOut = OracleLibrary.getQuoteAtTick(
            tick,
            uint128(amountIn),
            path[i],
            path[i + 1]
        );
        amountIn = amountOut;
    }
}
```

Recommendation

It is recommended to account for the fees of the swaps to ensure accurate `amountOut` calculations, especially in multi-hop scenarios. Each pool charges a fee, and failing to deduct these fees leads to overestimated returns, inefficient routing decisions.

ILU - Inconsistent Library Use

Criticality	Minor / Informative
Location	LpRouter.sol#L645
Status	Unresolved

Description

`_prepareExitPoolRequest` uses the `WeightedPoolUserData` library to `_prepareExitPoolRequest` when the `tokens.length` is equal to two. However in all other cases `StablePoolUserData` is used instead. This could create inconsistencies when trying to exit the pool.

```
request.userData = tokens.length == 2
    ?
    abi.encode(WeightedPoolUserData.ExitKind.EXACT_BPT_IN_FOR_TOKEN
    S_OUT, lpAmount)
    : abi.encode(

    StablePoolUserData.ExitKind.EXACT_BPT_IN_FOR_ONE_TOKEN_OUT,
        lpAmount,
        tokens.length - 2
    );
```

Recommendation

It is recommended to use a specific library for both entering and exiting a pool.

CR - Code Repetition

Criticality	Minor / Informative
Location	LpRouter.sol#L397,471,532
Status	Unresolved

Description

The contract contains repetitive code segments. There are potential issues that can arise when using code segments in Solidity. Some of them can lead to issues like gas efficiency, complexity, readability, security, and maintainability of the source code. It is generally a good idea to try to minimize code repetition where possible.

```
function _addLiquidityKodiak(  
    IKodiakVaultV1 lp,  
    address tokenIn,  
    uint256 amountIn,  
    address recipient,  
    address router  
) internal returns (uint256 tokenOutAmount) { /*...*/  
  
function _addLiquiditySteer(  
    ISushiMultiPositionLiquidityManager lp,  
    address tokenIn,  
    uint256 amountIn,  
    address recipient,  
    address router  
) internal returns (uint256 tokenOutAmount) { /*...*/  
  
function _addLiquidityGamma(  
    IHypervisor lp,  
    address tokenIn,  
    uint256 amountIn,  
    address recipient,  
    address router  
) internal returns (uint256 tokenOutAmount) { /*...*/
```

Recommendation

The team is advised to avoid repeating the same code in multiple places, which can make the contract easier to read and maintain. The authors could try to reuse code wherever possible, as this can help reduce the complexity and size of the contract. For instance, the contract could reuse the common code segments in an internal function in order to avoid repeating the same code in multiple places.

CCR - Contract Centralization Risk

Criticality	Minor / Informative
Location	controllers/Controller.sol#L154,163,172,217 vaults/Vault.sol#L195 StrategyFactoryBase.sol#L76,85,94,103,264 ZapperBase.sol#L117,127,138,149,159,170,181 InfraredZapper.sol#L164 LpRouter.sol#L70,78,87 SwapRouter.sol#L118,126,134,143,153,171
Status	Unresolved

Description

The contract's functionality and behavior are heavily dependent on external parameters or configurations. While external configuration can offer flexibility, it also poses several centralization risks that warrant attention. Centralization risks arising from the dependence on external configuration include Single Point of Control, Vulnerability to Attacks, Operational Delays, Trust Dependencies, and Decentralization Erosion.

```
function setGovernance(address governanceAddress) public
onlyGovernance sphereXGuardPublic(0xefc74f14, 0xab033ea9) {}

function setTimelock(address timelockAddress) public
onlyTimelock sphereXGuardPublic(0xdecf35e6, 0xbdacb303) {}

function setController(address controllerAddress) external
onlyTimelock sphereXGuardExternal(0x431250ca) {}

function setStrategist(address strategistAddress) public
onlyGovernance sphereXGuardPublic(0x15f23c15, 0xc7b9d530) {}

function setStrategy(
    address asset,
    address strategy
) public nonReentrant onlyStrategist
sphereXGuardPublic(0x632853be, 0x72cb5d97) {}

function setSphereXEngine(address sphereXEngineAddress)
external onlyDev {}

function setVaultFactory(address factoryAddress) external
onlyDev {}

function setControllerFactory(address factoryAddress)
external onlyDev {}

function createVault(
    VaultCreateParams calldata params
) external onlyDev onlyNewAsset(params.asset) returns (IVault
vault, IController controller, IStrategy strategy) {}

function setDev(address devAddress) external onlyDev {}

function setSwapRouter(address routerAddress) external
onlyGovernance sphereXGuardExternal(0xd473ef3c) {}

function setIpRouter(address routerAddress) external
onlyGovernance sphereXGuardExternal(0x26b2eef4) {}

function setStableCoin(address stablecoinAddress) external
onlyGovernance sphereXGuardExternal(0x5b9fdae4) {}

function setZapInFee(uint16 newFee) external onlyGovernance
{}

function setZapOutFee(uint16 newFee) external onlyGovernance
{}

function setFeeRecipient(address newRecipient) external
```

```
onlyGovernance {}

function setAssetInfo(address asset, bool isSingleToken,
IDexType.DexType dex) external onlyGovernance {}

function setRouter(uint8 dex, address router) external
onlyGovernance sphereXGuardExternal(0xa3f6b48c) {}

function setDefaultDex(uint8 dex) external onlyGovernance
sphereXGuardExternal(0x76f61bc5) {}

function setFactory(uint8 dex, address factory) external
onlyGovernance sphereXGuardExternal(0x93b83854) {}

function setPool(
    address tokenIn,
    address tokenOut,
    address pool
) external onlyGovernance sphereXGuardExternal(0x93b83854) {}

function setSwapRoute(
    address tokenIn,
    address tokenOut,
    SwapRoutePath[] memory path,
    bool reversePath
) external onlyGovernance sphereXGuardExternal(0x1a19f525) {}
```

Recommendation

To address this finding and mitigate centralization risks, it is recommended to evaluate the feasibility of migrating critical configurations and functionality into the contract's codebase itself. This approach would reduce external dependencies and enhance the contract's self-sufficiency. It is essential to carefully weigh the trade-offs between external configuration flexibility and the risks associated with centralization.

ELFM - Exceeds Fees Limit

Criticality	Minor / Informative
Location	StrategyBase.sol#L27
Status	Unresolved

Description

The contract timelock address has the authority to increase performance fees over the allowed limit of 25%. The timelock address may take advantage of it by calling the `setPerformanceDevFee` or `setPerformanceTreasuryFee` function with a high percentage value.

```
function setPerformanceDevFee(uint16 fee) external onlyTimelock
sphereXGuardExternal(0x39189706) {
    if (fee + performanceTreasuryFee > MAX_PERFORMANCE_FEE)
revert FeeTooHigh(fee, MAX_PERFORMANCE_FEE);
    uint16 old = performanceDevFee;
    performanceDevFee = fee;
    emit PerformanceDevFeeChanged(old, fee);
}

function setPerformanceTreasuryFee(uint16 fee) external
onlyTimelock sphereXGuardExternal(0x76672d92) {
    if (fee + performanceDevFee > MAX_PERFORMANCE_FEE) revert
FeeTooHigh(fee, MAX_PERFORMANCE_FEE);
    uint16 old = performanceTreasuryFee;
    performanceTreasuryFee = fee;
    emit PerformanceTreasuryFeeChanged(old, fee);
}
```

Recommendation

The contract could embody a check for the maximum acceptable value. The team should carefully manage the private keys of the timelock's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions.

Temporary Solutions:

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

GRLNS - Gamma Remove Liquidity Not Supported

Criticality	Minor / Informative
Location	LpRouter.sol#L118
Status	Unresolved

Description

`LpRouter` does not support removing liquidity for the `DexType.GAMMA`. Since `LpRouter` allows for adding liquidity to a `GAMMA` `DexType` there should also be functionality for removing it.

```
function removeLiquidity(
    address lp,
    uint256 lpAmount,
    address recipient,
    address tokenOut,
    DexType dexType
) public override nonReentrant sphereXGuardPublic(0xd04d32ff,
0x31512b67) returns (uint256 tokenOutAmount) {
    address router = routers[uint8(dexType)];
    if (dexType == DexType.BEX) {
        return _removeLiquidityBex(IBeraPool(lp), lpAmount,
recipient, tokenOut);
    } else if (dexType == DexType.STEER) {
        return
_removeLiquiditySteer(ISushiMultiPositionLiquidityManager(lp),
lpAmount, recipient, tokenOut);
    } else if (dexType == DexType.KODIAK_V3) {
        return _removeLiquidityKodiak(IKodiakVaultV1(lp),
lpAmount, recipient, router, tokenOut);
    } else {
        revert UnsupportedDexType();
    }
}
```

Recommendation

The team should consider adding support for removing liquidity for `DexType.GAMMA`.

MC - Missing Check

Criticality	Minor / Informative
Location	SwapRouter.sol#L69
Status	Unresolved

Description

The contract is processing variables that have not been properly sanitized and checked that they form the proper shape. These variables may produce vulnerability issues.

Specifically, a check is missing to ensure that `balancerQueriesAddress` is not `address(0)`

```
balancerQueries = balancerQueriesAddress;
```

Recommendation

The team is advised to properly check the variables according to the required specifications.

MN - Misspelled Naming

Criticality	Minor / Informative
Location	SwapRouter.sol#L171
Status	Unresolved

Description

The contract is designed to manage swap routes through the `setSwapRoute` function. However, within this function, the word "route" is used instead of "router". This misspelling may cause confusion for developers and users interacting with the code, as it deviates from the expected terminology used to describe swap routes. While this does not directly affect the functionality of the contract, it may reduce readability and increase the likelihood of misunderstandings or mistakes during future development or maintenance.

```
function setSwapRoute(
  address tokenIn,
  address tokenOut,
  SwapRoutePath[] memory path,
  bool reversePath
) external onlyGovernance sphereXGuardExternal(0x1a19f525) {
  SwapRoutePath[] storage swapRouteForward =
  swapRoutes[tokenIn][tokenOut];
  if (swapRouteForward.length > 0) delete
  swapRoutes[tokenIn][tokenOut];
  for (uint256 i = 0; i < path.length; i++) {
    swapRouteForward.push(path[i]);
    // if the pool is available, set the pool for the token
    pair
    //..
  }

  if (reversePath) {
    SwapRoutePath[] storage swapRouteReverse =
    swapRoutes[tokenOut][tokenIn];
    if (swapRouteReverse.length > 0) delete
    swapRoutes[tokenOut][tokenIn];
    for (uint256 i = 0; i < path.length; i++) {
      SwapRoutePath memory inversePath = path[path.length - i -
1];
      swapRouteReverse.push(
        SwapRoutePath({
          tokenIn: inversePath.tokenOut,
          tokenOut: inversePath.tokenIn,
          dex: inversePath.dex,
          isMultiPath: inversePath.isMultiPath,
          pool: inversePath.pool
        })
      );
    }
  }
  emit SetSwapRoute(tokenIn, tokenOut, path, reversePath);
}
```

Recommendation

It is recommended to correct the misspelled names to align with the intended term "router". Consistent and accurate naming conventions enhance code readability, maintainability, and the overall clarity of the contract. Adhering to clear naming practices reduces potential misinterpretation by developers and auditors.

ORA - Overwriting Rewards Amount

Criticality	Minor / Informative
Location	InfraredStrategy.sol#L108
Status	Unresolved

Description

`harvest` function loops through the `rewardTokensLength` to find a `rewardToken` that is equal to the address of the `asset`. However if multiple `rewardToken` have this address then only the last one will be harvested since `newAssets` is getting overwritten.

```
for (uint256 i = 0; i < rewardTokensLength; i++) {
    address rewardToken = staking.rewardTokens(i);
    uint256 rewardAmount =
    IERC20(rewardToken).balanceOf(address(this));
    if (rewardToken == address(asset)) {
        newAssets = rewardAmount;
    } else if (rewardAmount > 0 && rewardToken != wrappedNative)
    {
        IERC20(rewardToken).safeTransfer(address(swapRouter),
        rewardAmount);
        swapRouter.swapWithDefaultDex(rewardToken, wrappedNative,
        rewardAmount, 0, address(this));
    }
}
```

Recommendation

The team could consider adding the amount instead of overwriting it. In that case, the `harvest` function will account for all the possible `asset` tokens instead of the last one.

PZAZI - Possible Zero Amount Zap In

Criticality	Minor / Informative
Location	ArberaZapper.sol#L462,463
Status	Unresolved

Description

In the `zapIn` function the `assetsIn` is approved and deposited in the `vault`. If the `vaults.asset()` is the `tokenIn` it will not make the swap and `assetsIn` will stay zero. This means that `zapIn` will `approve` and send to the `vault` zero tokens.

```
uint256 assetsIn;
if (vault.asset() != tokenIn) {
    (assetsIn, returnedAssets) = swapToAssets(vault.asset(),
tokenIn, tokenInAmount, address(this));
}

// approve the asset to the vault
IERC20(vault.asset()).forceApprove(address(vault), assetsIn);

// deposit the asset to the vault
shares = vault.deposit(assetsIn, msg.sender, minShares);
```

Recommendation

It is recommended to account for the case of `vault.asset()` being the `tokenIn` and make `assetsIn` equal to the `tokenInAmount`.

PLPI - Potential Liquidity Provision Inadequacy

Criticality	Minor / Informative
Location	utils/SwapRouter.sol#L447,515,563,606,640,675
Status	Unresolved

Description

The contract operates under the assumption that liquidity is consistently provided to the pair between the contract's token and the native currency. However, there is a possibility that liquidity is provided to a different pair. This inadequacy in liquidity provision in the main pair could expose the contract to risks. Specifically, during eligible transactions, where the contract attempts to swap tokens with the main pair, a failure may occur if liquidity has been added to a pair other than the primary one. Consequently, transactions triggering the swap functionality will result in a revert.

```
function _swapWithRoute(
    address tokenIn,
    address tokenOut,
    uint256 amountIn,
    uint256 amountOutMinimum,
    address recipient
) internal sphereXGuardInternal(0xf01e8b19) returns (uint256
amountOut) {}

function _swapBex(
    address tokenIn,
    address tokenOut,
    uint256 amountIn,
    uint256 amountOutMinimum,
    address recipient,
    IBeraPool pool
) internal returns (uint256 amountOut) {}

function _swapV3(
    address tokenIn,
    address tokenOut,
    uint256 amountIn,
    uint256 amountOutMinimum,
    address recipient,
    address router,
    address factory
) internal sphereXGuardInternal(0xd2c5d247) returns (uint256
amountOut) {}

function _swapV3WithPath(
    address[] memory path,
    uint256 amountIn,
    uint256 amountOutMinimum,
    address recipient,
    address router,
    address factory
) internal sphereXGuardInternal(0x7d29fbe4) returns (uint256
amountOut) {}

function _swapV2(
    address tokenIn,
    address tokenOut,
    uint256 amountIn,
    uint256 amountOutMinimum,
    address recipient,
    address router
) internal sphereXGuardInternal(0xd8b71976) returns (uint256
amountOut) {}
```

```
function _swapV2WithPath(  
    address[] memory path,  
    uint256 amountIn,  
    uint256 amountOutMinimum,  
    address recipient,  
    address router  
) internal sphereXGuardInternal(0x0de072e7) returns (uint256  
amountOut) {}
```

Recommendation

The team is advised to implement a runtime mechanism to check if the pair has adequate liquidity provisions. This feature allows the contract to omit token swaps if the pair does not have adequate liquidity provisions, significantly minimizing the risk of potential failures.

Furthermore, the team could ensure the contract has the capability to switch its active pair in case liquidity is added to another pair.

Additionally, the contract could be designed to tolerate potential reverts from the swap functionality, especially when it is a part of the main transfer flow. This can be achieved by executing the contract's token swaps in a non-reversible manner, thereby ensuring a more resilient and predictable operation.

SAU - Swapped Amount Uninitialized

Criticality	Minor / Informative
Location	LpRouter.sol#L289
Status	Unresolved

Description

`handleTokenSwaps` is used to swap `tokenIn` to a token that can be used to provide liquidity to a specified `lp`. However if either of the initial amounts added is zero or when more than two tokens are added as input the entire contract's balance of `tokenIn` is used to calculate the `swappedAmount1`. The `swappedAmount0` is not calculated, therefore it will always be zero.

Additionally, in case of having more than two tokens in the `tokens` array, only the last token will be handled.

```
{
    uint256 tokenInBalance =
    IERC20(tokenIn).balanceOf(address(this));
    if (address(tokenIn) != lastToken) {
        IERC20(tokenIn).safeTransfer(address(swapRouter),
        tokenInBalance);
        swappedAmount1 = swapRouter.swapWithDefaultDex(tokenIn,
        lastToken, tokenInBalance, 0, address(this));
    } else {
        swappedAmount1 = tokenInBalance;
    }
}
```

Recommendation

The team is advised to consider the situations that can occur when trying to provide liquidity with zero amounts of tokens.

USV - Uninitialized State Variable

Criticality	Minor / Informative
Location	Vault.sol#L50
Status	Unresolved

Description

In the `Vault` contract, there is an address state variable declared as `feeRecipient` but there is no functionality that provides a valid address for it. This results in the `feeRecipient` to always be `address(0)`.

```
address public feeRecipient;
```

Recommendation

To prevent `feeRecipient` from defaulting to `address(0)`, if not intended, it is recommended to add the functionality needed to set it with a valid address.

UBUFL - Unintended Balance Used For Liquidity

Criticality	Minor / Informative
Location	LpRouter.sol#L93
Status	Unresolved

Description

The contract declares `addLiquidity` as a public function. Additionally, `addLiquidity` does not transfer tokens from the user to the contract but instead assumes that they are provided beforehand. This can create situations where users provide tokens in the contract and the tokens are used before they use `addLiquidity`. Since users are able to choose the `amountIn` they could use any amount of tokens stored in the contract. Additionally, excess tokens will be returned to the caller.

```
function addLiquidity(
    address lp,
    address tokenIn,
    uint256 amountIn,
    address recipient,
    DexType dexType
) public nonReentrant sphereXGuardPublic(0xed92e336,
0xee52e659) returns (uint256 lpAmountOut) {
    //...
}
```

Additionally in `_addLiquidityBex` if `amountIn` is zero or one then `_handleTokenSwaps` will return `amount1` calculated by the entire contract's balance.

```
function _addLiquidityBex(
    IBeraPool lp,
    address tokenIn,
    uint256 amountIn,
    address recipient
) internal sphereXGuardInternal(0x6a9e79f4) returns (uint256
lpAmountOut) {
    //...
    (amount0, amount1) = _handleTokenSwaps(tokenIn, tokens,
amount0, amount1);
    //...
}

function _handleTokenSwaps(
    address tokenIn,
    IERC20[] memory tokens,
    uint256 amount0,
    uint256 amount1
) internal returns (uint256 swappedAmount0, uint256
swappedAmount1) {
    if (amount0 > 0 && amount1 > 0) {
        //...
    } else {
        //get balance of tokenIn
        uint256 tokenInBalance =
IERC20(tokenIn).balanceOf(address(this));

        // Handle last token
        if (address(tokenIn) != lastToken) {
            IERC20(tokenIn).safeTransfer(address(swapRouter),
tokenInBalance);
            swappedAmount1 =
swapRouter.swapWithDefaultDex(tokenIn, lastToken,
tokenInBalance, 0, address(this));
        } else {
            swappedAmount1 = tokenInBalance;
        }
    }
}
```

Recommendation

The team could consider using a strategy that allows users to first approve the tokens to the `LpRouter` and then use `addLiquidity` to utilize only the approved amount.

UTPD - Unverified Third Party Dependencies

Criticality	Minor / Informative
Location	strategies/StrategyBase.sol#L192 strategies/InfraredStrategy.sol#L79 StrategyFactoryBase.sol#L168 LpRouter.sol#L522,610
Status	Unresolved

Description

The contract uses an external contract in order to determine the transaction's flow. The external contract is untrusted. As a result, it may produce security issues and harm the transactions.

```
function _swapBGTToAsset() internal returns (uint256 amount) {
    uint256 balance = IERC20(bgt).balanceOf(address(this));
    if (balance > 0) {
        bgt.redeem(address(this), balance);
        ...
    }
    ...
}
```

```
function deposit() public override {
    ...
    staking.stake(balance);
}
```

```
address public sphereXEngine;
...
ISphereXEngine(sphereXEngine).addAllowedSenderOnChain(address(controller));
ISphereXEngine(sphereXEngine).addAllowedSenderOnChain(address(vault));
};
```



```
...  
ISteerPeriphery(router).deposit(address(lp),  
liquidityInfo.amount0, liquidityInfo.amount1, 0, 0,  
address(this));  
...  
lp.withdraw(lpAmount, 0, 0, address(this));
```

Recommendation

The contract should use a trusted external source. A trusted source could be either a commonly recognized or an audited contract. The pointing addresses should not be able to change after the initialization.

L02 - State Variables could be Declared Constant

Criticality	Minor / Informative
Location	Vault.sol#L50
Status	Unresolved

Description

State variables can be declared as constant using the constant keyword. This means that the value of the state variable cannot be changed after it has been set. Additionally, the constant variables decrease gas consumption of the corresponding transaction.

```
address public feeRecipient
```

Recommendation

Constant state variables can be useful when the contract wants to ensure that the value of a state variable cannot be changed by any function in the contract. This can be useful for storing values that are important to the contract's behavior, such as the contract's address or the maximum number of times a certain function can be called. The team is advised to add the constant keyword to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	ArberaStrategy.sol#L128
Status	Unresolved

Description

The Solidity style guide is a set of guidelines for writing clean and consistent Solidity code. Adhering to a style guide can help improve the readability and maintainability of the Solidity code, making it easier for others to understand and work with.

The followings are a few key points from the Solidity style guide:

1. Use camelCase for function and variable names, with the first letter in lowercase (e.g., myVariable, updateCounter).
2. Use PascalCase for contract, struct, and enum names, with the first letter in uppercase (e.g., MyContract, UserStruct, ErrorEnum).
3. Use uppercase for constant variables and enums (e.g., MAX_VALUE, ERROR_CODE).
4. Use indentation to improve readability and structure.
5. Use spaces between operators and after commas.
6. Use comments to explain the purpose and behavior of the code.
7. Keep lines short (around 120 characters) to improve readability.

```
address _rewardToken
```

Recommendation

By following the Solidity naming convention guidelines, the codebase increased the readability, maintainability, and makes it easier to work with.

Find more information on the Solidity documentation

<https://docs.soliditylang.org/en/stable/style-guide.html#naming-conventions>.

L09 - Dead Code Elimination

Criticality	Minor / Informative
Location	ZapperBase.sol#L203,232,249
Status	Unresolved

Description

In Solidity, dead code is code that is written in the contract, but is never executed or reached during normal contract execution. Dead code can occur for a variety of reasons, such as:

- Conditional statements that are always false.
- Functions that are never called.
- Unreachable code (e.g., code that follows a return statement).

Dead code can make a contract more difficult to understand and maintain, and can also increase the size of the contract and the cost of deploying and interacting with it.

```
function _approveTokenIfNeeded(  
    address tokenAddress,  
    address spenderAddress  
) internal sphereXGuardInternal(0x367a5b5d) {  
    if (IERC20(tokenAddress).allowance(address(this),  
spenderAddress) == 0) {  
        IERC20(tokenAddress).approve(spenderAddress,  
type(uint256).max);  
    }  
}
```

Recommendation

To avoid creating dead code, it's important to carefully consider the logic and flow of the contract and to remove any code that is not needed or that is never executed. This can help improve the clarity and efficiency of the contract.

L14 - Uninitialized Variables in Local Scope

Criticality	Minor / Informative
Location	LpRouter.sol#L370,371,404,478,539,605,621 ArberaZapper.sol#L462,514
Status	Unresolved

Description

Using an uninitialized local variable can lead to unpredictable behavior and potentially cause errors in the contract. It's important to always initialize local variables with appropriate values before using them.

```
uint256 amount0  
uint256 amount1  
LiquidityAddInfo memory liquidityInfo  
LiquidityRemoveInfo memory liquidityInfo  
uint256 assetsIn
```

Recommendation

By initializing local variables before using them, the contract ensures that the functions behave as expected and avoid potential issues.

L15 - Local Scope Variable Shadowing

Criticality	Minor / Informative
Location	SteerZapper.sol#L31,32,33,34,35,36,37 KodiakZapper.sol#L31,33,34,35,36,37 interfaces/IController.sol#L105,108,111 InfraredZapper.sol#L27,28,29,30,31,32,33 ArberaZapper.sol#L26,27,28,29,30,31,32
Status	Unresolved

Description

Local scope variable shadowing occurs when a local variable with the same name as a variable in an outer scope is declared within a function or code block. When this happens, the local variable "shadows" the outer variable, meaning that it takes precedence over the outer variable within the scope in which it is declared.

```
address wrappedNative
address stablecoin
address swapRouter
address lpRouter
address feeRecipient
uint16 zapInFee
uint16 zapOutFee
address strategist
address governance
address timelock
```

Recommendation

It's important to be aware of shadowing when working with local variables, as it can lead to confusion and unintended consequences if not used correctly. It's generally a good idea to choose unique names for local variables to avoid shadowing outer variables and causing confusion.

L17 - Usage of Solidity Assembly

Criticality	Minor / Informative
Location	StrategyFactoryBase.sol#L309 StrategyBase.sol#L437
Status	Unresolved

Description

Using assembly can be useful for optimizing code, but it can also be error-prone. It's important to carefully test and debug assembly code to ensure that it is correct and does not contain any errors.

Some common types of errors that can occur when using assembly in Solidity include Syntax, Type, Out-of-bounds, Stack, and Revert.

```
assembly {
    strategyAddress := create(0, add(bytecode, 0x20),
mload(bytecode))

    if iszero(extcodesize(strategyAddress)) {
        revert(0, 0)
    }
}
...
```

Recommendation

It is recommended to use assembly sparingly and only when necessary, as it can be difficult to read and understand compared to Solidity code.

Functions Analysis

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
ZapperBase	Implementation	SphereXProtected, ReentrancyGuard, IZapper		
		Public	✓	-
	setGovernance	External	✓	onlyGovernance
	setSwapRouter	External	✓	onlyGovernance sphereXGuardExternal
	setLpRouter	External	✓	onlyGovernance sphereXGuardExternal
	setStableCoin	External	✓	onlyGovernance sphereXGuardExternal
	setZapInFee	External	✓	onlyGovernance
	setZapOutFee	External	✓	onlyGovernance
	setFeeRecipient	External	✓	onlyGovernance
		External	Payable	-
	_revertAddressZero	Internal		
	_approveTokenIfNeeded	Internal	✓	sphereXGuardInternal
	_safeTransferFromTokens	Internal	✓	sphereXGuardInternal
	_divideAmountInRatio	Internal		

	_returnAssets	Internal	✓	sphereXGuardInternal
	_returnAsset	Internal	✓	sphereXGuardInternal
	_returnAssetWithAmount	Internal	✓	
	_transferFee	Internal	✓	
	swapToAssets	Public	✓	-
	swapFromAssets	Public	✓	-
	zapIn	External	Payable	nonReentrant sphereXGuardExternal
	zapOut	External	✓	nonReentrant sphereXGuardExternal
VaultFactory	Implementation	SphereXProtectedBase, IVaultFactory		
		Public	✓	SphereXProtectedBase
	_revertAddressZero	Internal		
	setDev	External	✓	onlyDev sphereXGuardExternal
	setWhitelistedStrategyFactory	External	✓	onlyDev sphereXGuardExternal
	setSphereXProtected	Private	✓	sphereXGuardInternal
	createVault	External	✓	onlyWhitelisted StrategyFactory sphereXGuardExternal
Vault	Implementation	SphereXProtected, ReentrancyGuard,		

		ERC4626, IVault		
		Public	✓	ERC4626 ERC20
	_revertOnlyGovernance	Internal		
	_revertOnlyTimelock	Internal		
	_revertOnlyController	Internal		
	_revertAddressZero	Internal		
	decimals	Public		-
	setMin	External	✓	onlyGovernanc e sphereXGuardE xternal
	setDepositFee	External	✓	onlyGovernanc e
	setWithdrawFee	External	✓	onlyGovernanc e
	setGovernance	External	✓	onlyGovernanc e sphereXGuardE xternal
	setTimelock	External	✓	onlyTimelock sphereXGuardE xternal
	setController	External	✓	onlyTimelock sphereXGuardE xternal
	available	Public		-
	totalAssets	Public		-
	earn	Public	✓	nonReentrant sphereXGuardP ublic
	harvest	External	✓	nonReentrant onlyController sphereXGuardE xternal
	_withdraw	Internal	✓	sphereXGuardI nternal

	_deposit	Internal	✓	sphereXGuardInternal
	deposit	Public	✓	nonReentrant sphereXGuardPublic
	redeem	Public	✓	nonReentrant sphereXGuardPublic
SwapRouter	Implementation	SphereXProtected, ReentrancyGuard, ISwapRouter		
		Public	✓	-
	validateSwapParams	Internal		
	validateSwapWithPathParams	Internal		
	setGovernance	Public	✓	onlyGovernance sphereXGuardPublic
	setDefaultDex	External	✓	onlyGovernance sphereXGuardExternal
	setRouter	External	✓	onlyGovernance sphereXGuardExternal
	setFactory	External	✓	onlyGovernance sphereXGuardExternal
	setPool	External	✓	onlyGovernance sphereXGuardExternal
	setSwapRoute	External	✓	onlyGovernance sphereXGuardExternal
	swapWithDefaultDex	External	✓	resetPathLength

				sphereXGuardE xternal
	swap	Public	✓	nonReentrant sphereXGuardP ublic
	swapWithPathWithDefaultDex	Public	✓	nonReentrant sphereXGuardP ublic
	swapWithPath	Public	✓	nonReentrant sphereXGuardP ublic
	getQuoteWithDefaultDex	External	✓	-
	getQuote	Public	✓	-
	getQuoteWithPathWithDefaultDex	External		-
	getQuoteWithPath	Public		-
	_revertAddressZero	Internal		
	_revertZeroAmount	Internal		
	_revertInvalidPathLength	Internal		
	_findMostLiquidV3Pool	Internal		
	_swapWithRoute	Internal	✓	sphereXGuardI nternal
	_swapBex	Internal	✓	
	_swapV3	Internal	✓	sphereXGuardI nternal
	_swapV3WithPath	Internal	✓	sphereXGuardI nternal
	_swapV2	Internal	✓	sphereXGuardI nternal
	_swapV2WithPath	Internal	✓	sphereXGuardI nternal
	_getQuoteV3	Internal		
	_getQuoteV3WithPath	Internal		
	_getBexQuote	Internal	✓	

	_getQuoteV2	Internal		
	_getQuoteV2WithPath	Internal		
StrategyFactoryBase	Implementation	IStrategyFactory		
		Public	✓	-
	revertOnlyDev	Private		
	_revertAddressZero	Internal		
	setDev	External	✓	onlyDev
	setSphereXEngine	External	✓	onlyDev
	setVaultFactory	External	✓	onlyDev
	setControllerFactory	External	✓	onlyDev
	_setAddressAsSpherexProtected	Internal	✓	
	_createControllerAndVault	Internal	✓	
	_setupVault	Internal	✓	
	revertIfNonInitializedParams	Private		
	_encodeParamsAndController	Private		
	createVault	External	✓	onlyDev onlyNewAsset
	_deployStrategyByteCode	Internal	✓	
StrategyBase	Implementation	SphereXProtected, ReentrancyGuard, IStrategy		
		Public	✓	-
		External	Payable	-
	balanceOfAsset	Public		-

	balanceOfPool	Public		-
	balanceOf	Public		-
	_revertAddressZero	Internal		
	_revertOnlyGovernance	Internal		
	_revertOnlyTimelock	Internal		
	_revertOnlyController	Internal		
	_revertOnlyBenevolent	Internal		
	_swapBGTToAsset	Internal	✓	sphereXGuardInternal
	whitelistHarvester	External	✓	sphereXGuardExternal onlyBenevolent
	revokeHarvester	External	✓	sphereXGuardExternal onlyBenevolent
	setWithdrawalDevFundFee	External	✓	onlyTimelock sphereXGuardExternal
	setWithdrawalTreasuryFee	External	✓	onlyTimelock sphereXGuardExternal
	setPerformanceDevFee	External	✓	onlyTimelock sphereXGuardExternal
	setPerformanceTreasuryFee	External	✓	onlyTimelock sphereXGuardExternal
	setStrategist	External	✓	onlyGovernance sphereXGuardExternal
	setGovernance	External	✓	onlyGovernance sphereXGuardExternal
	setTimelock	External	✓	onlyTimelock sphereXGuardExternal

	setController	External	✓	onlyTimelock sphereXGuardE xternal
	setSwapRouter	External	✓	onlyGovernanc e sphereXGuardE xternal
	setLpRouter	External	✓	onlyGovernanc e sphereXGuardE xternal
	setZapper	External	✓	onlyGovernanc e sphereXGuardE xternal
	deposit	Public	✓	-
	getHarvestable	External		-
	harvest	Public	✓	nonReentrant onlyBenevolent sphereXGuardP ublic
	_withdrawSome	Internal	✓	
	withdraw	External	✓	nonReentrant onlyController sphereXGuardE xternal
	withdraw	External	✓	nonReentrant onlyController sphereXGuardE xternal
	withdrawForSwap	External	✓	nonReentrant onlyController sphereXGuardE xternal
	withdrawAll	External	✓	nonReentrant onlyController sphereXGuardE xternal
	_withdrawAll	Internal	✓	sphereXGuardI nternal
	execute	Public	Payable	onlyTimelock sphereXGuardP ublic

	_distributePerformanceFeesBasedAmountAndDeposit	Internal	✓	sphereXGuardInternal
SteerZapper	Implementation	ZapperBase		
		Public	✓	ZapperBase
	swapToAssets	Public	✓	sphereXGuardPublic
	swapFromAssets	Public	✓	sphereXGuardPublic
SteerStrategy	Implementation	StrategyBase		
		Public	✓	StrategyBase
	deposit	Public	✓	sphereXGuardPublic
	balanceOfPool	Public		-
	_withdrawSome	Internal	✓	sphereXGuardInternal
SteerFactory	Implementation	StrategyFactoryBase		
		Public	✓	StrategyFactoryBase
	createVaultWithParams	External	✓	onlyDev onlyNewAsset
LpRouter	Implementation	SphereXProtected, ReentrancyGuard, ILpRouter		
		Public	✓	-
	setGovernance	Public	✓	onlyGovernance

				sphereXGuardPublic
	setSwapRouter	External	✓	onlyGovernance sphereXGuardExternal
	setRouter	External	✓	onlyGovernance sphereXGuardExternal
	addLiquidity	Public	✓	nonReentrant sphereXGuardPublic
	removeLiquidity	Public	✓	nonReentrant sphereXGuardPublic
	_revertAddressZero	Internal		
	_returnAssets	Internal	✓	
	_approveTokenIfNeeded	Internal	✓	sphereXGuardInternal
	_divideAmountInRatio	Internal		
	_getAmountsForLiquidityInRatio	Internal	✓	
	_handleRemainingTokens	Internal	✓	
	_handleTokenSwaps	Internal	✓	
	_prepareJoinPoolRequest	Internal		
	_addLiquidityBex	Internal	✓	sphereXGuardInternal
	_addLiquidityKodiak	Internal	✓	
	_addLiquiditySteer	Internal	✓	
	_addLiquidityGamma	Internal	✓	
	_removeLiquiditySteer	Internal	✓	
	_removeLiquidityKodiak	Internal	✓	
	_prepareExitPoolRequest	Internal		

	_removeLiquidityBex	Internal	✓	sphereXGuardInternal
KodiakZapper	Implementation	ZapperBase		
		Public	✓	ZapperBase
	swapToAssets	Public	✓	sphereXGuardPublic
	swapFromAssets	Public	✓	sphereXGuardPublic
KodiakStrategy	Implementation	StrategyBase		
		Public	✓	StrategyBase
	deposit	Public	✓	sphereXGuardPublic
	balanceOfPool	Public		-
	_withdrawSome	Internal	✓	sphereXGuardInternal
KodiakFactory	Implementation	StrategyFactoryBase		
		Public	✓	StrategyFactoryBase
	createVaultWithParams	External	✓	onlyDev onlyNewAsset
InfraredZapper	Implementation	ZapperBase		
		Public	✓	ZapperBase
	swapToAssets	Public	✓	sphereXGuardPublic
	_swapToAssetsLp	Internal	✓	

	swapFromAssets	Public	✓	sphereXGuardPublic
	_swapFromAssetsLp	Internal	✓	
	setAssetInfo	External	✓	onlyGovernance
InfraredStrategy	Implementation	StrategyBase		
		Public	✓	StrategyBase
	deposit	Public	✓	nonReentrant sphereXGuardPublic
	getHarvestable	External		-
	harvest	Public	✓	onlyBenevolent sphereXGuardPublic
	balanceOfPool	Public		-
	_withdrawSome	Internal	✓	sphereXGuardInternal
	setRewardTokensLength	External	✓	onlyGovernance sphereXGuardExternal
	setStaking	External	✓	onlyGovernance
InfraredFactory	Implementation	StrategyFactoryBase		
		Public	✓	StrategyFactoryBase
	deployStrategyWithParamsAndController	Internal	✓	
	createVaultWithParams	External	✓	onlyDev onlyNewAsset

ControllerFactory	Implementation	SphereXProtectedBase, IControllerFactory		
		Public	✓	SphereXProtectedBase
	_revertAddressZero	Internal		
	setDev	External	✓	onlyDev sphereXGuardExternal
	setWhitelistedStrategyFactory	External	✓	onlyDev sphereXGuardExternal
	setSphereXProtected	Private	✓	sphereXGuardInternal
	createController	External	✓	onlyWhitelistedStrategyFactory sphereXGuardExternal
Controller	Implementation	SphereXProtected, ReentrancyGuard, IController		
		Public	✓	-
	_revertAddressZero	Internal		
	_revertOneAddressZero	Internal		
	_revertOnlyGovernance	Internal		
	_revertOnlyStrategist	Internal		
	_revertOnlyTimelock	Internal		
	setDevFund	Public	✓	onlyGovernance sphereXGuardPublic
	setTreasury	Public	✓	onlyGovernance sphereXGuardPublic


	setStrategist	Public	✓	onlyGovernance sphereXGuardPublic
	setGovernance	Public	✓	onlyGovernance sphereXGuardPublic
	setTimelock	Public	✓	onlyTimelock sphereXGuardPublic
	setVault	Public	✓	onlyStrategist sphereXGuardPublic
	approveStrategy	Public	✓	onlyTimelock sphereXGuardPublic
	revokeStrategy	Public	✓	onlyGovernance sphereXGuardPublic
	setStrategy	Public	✓	nonReentrant onlyStrategist sphereXGuardPublic
	earn	Public	✓	nonReentrant sphereXGuardPublic
	balanceOf	External		-
	withdrawAll	Public	✓	nonReentrant onlyStrategist sphereXGuardPublic
	inCaseTokensGetStuck	Public	✓	onlyGovernance sphereXGuardPublic
	inCaseStrategyTokenGetStuck	Public	✓	onlyGovernance sphereXGuardPublic
	withdraw	Public	✓	nonReentrant onlyVault sphereXGuardPublic

ArberaZapper	Implementation	ZapperBase		
		Public	✓	ZapperBase
	swapToAssets	Public	✓	sphereXGuardPublic
	swapFromAssets	Public	✓	sphereXGuardPublic
	swapToAssetsWithBond	Public	✓	sphereXGuardPublic
	swapFromAssetsWithBond	Public	✓	sphereXGuardPublic
	_getAmounts	Internal		
	zapIn	External	Payable	nonReentrant sphereXGuardExternal
	zapInWithBond	External	Payable	nonReentrant sphereXGuardExternal
	zapOutWithBond	External	✓	nonReentrant sphereXGuardExternal
ArberaStrategy	Implementation	StrategyBase		
		Public	✓	StrategyBase
	deposit	Public	✓	sphereXGuardPublic
	getHarvestable	External		-
	harvest	Public	✓	onlyBenevolent sphereXGuardPublic
	balanceOfPool	Public		-
	_withdrawSome	Internal	✓	sphereXGuardInternal
	setRewardToken	External	✓	onlyGovernance

ArberaFactory	Implementation	StrategyFactoryBase		
		Public	✓	StrategyFactoryBase
	createVaultWithParams	External	✓	onlyDev onlyNewAsset

Inheritance Graph

For the detailed graph file, please refer to the following link:

 [Inheritance Graph.png](#)

Summary

The BeraTrax protocol implements a modular and secure yield-generation mechanism through its core components, Vaults, Controllers, Strategies, Factories, and Zappers. This audit investigates security vulnerabilities, evaluates business logic consistency, and identifies potential improvements to enhance system robustness and operational efficiency.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. 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 Cyberscope's prior written consent. 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 regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document 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 represents an extensive assessment 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. Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security. Cyberscope'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 Cyberscope are subject to dependencies and are 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.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.



The Cyberscope team

cyberscope.io