



Stabilitytics.fi

Live Infrastructure Audit

**Maple Finance /
Syrup**



PUBLIC LIA REPORT (UNSOLICITED)

Maple Finance / Syrup

Roles · Signers · Integrations — the live deployment, not the code.

ENGAGEMENT	ISSUED	VERSION	VERIFIED ON-CHAIN
LIA-2026-003	2026-07-15	v1.0	2026-07-15 · Ethereum block 25,537,989 · Base block 48,664,172 (via Etherscan v2)

FINAL

PILLAR 1

PILLAR 2

PILLAR 3

0 CRITICAL

0 HIGH

4 MEDIUM

2 LOW

2 INFO

CONTENTS

Table of contents

01	Executive summary	4
02	Engagement context	5
03	Scope reviewed	6
04	Security posture	8
05	Severity definitions	9
06	Status definitions	10
07	Findings summary	11
08	Roles & power distribution	12
09	Signer trust analysis	25
10	Third-party integrations	28
11	Audit findings	30
12	Centralisation & power concentration	38
13	Remediation roadmap	39
14	Conclusion	40
15	Methodology	41
16	Disclaimer & scope limits	42
17	About Stabilitytics	43

SECTION 01

Executive summary

Stabilitytics reviewed the live Maple Finance / Syrup deployment across Ethereum and Base — 77 contracts spanning governance, the version factories, the five active pools, and the cross-chain surface — on 2026-07-15 (Ethereum block 25,537,989; Base block 48,664,172). The Ethereum core is well-governed: upgrades and privileged parameter changes are registered and executed through an on-chain GovernorTimelock, the top-level authority is an independent 4-of-7 Safe, and the security and operational admins are 3-of-6 and 3-of-5 multisigs.

The material findings are cross-chain and operational. Base replicates the governance roles but not their safeguards: the Base upgrade authority (MapleGlobals governor and proxy admin) is a 3-of-5 Safe with no timelock, and the Base treasury is a 1-of-1 Safe. On Ethereum, the four active pool delegates — which configure pools and fund loans from pool liquidity — are each single externally-owned keys, and two singletons (PoolPermissionManager, BorrowerActions) upgrade outside the timelock. None is a critical on-chain theft vector: borrower validation is Governor-gated and the governance Safes are honest-majority, so these are key-management and defense-in-depth gaps rather than acute vulnerabilities.

Signer analysis found 22 distinct signers across six governance Safes with reasonable separation — the 4-of-7 daoMultisig has an independent set — though emergency-pause authority is a single shared team across both chains and two powered roles sit at 2-of-N. On the integration side, the Syrup LayerZero OFT delegate is correctly set to a multisig on both chains (not the unset / single-DVN failure mode), but its DVN verification stack still needs the LZCheck read to rate, and a legacy Chainlink CCIP receiver should be confirmed decommissioned. Every finding has a concrete, low-effort remediation; none requires a redesign.

SECTION 02

Engagement context

PROTOCOL Maple Finance / Syrup	ENGAGEMENT ID LIA-2026-003
ENGAGEMENT TYPE Public LIA report (unsolicited)	NETWORKS Ethereum · Base
SOURCE On-chain deployment (Ethereum + Base) + public documentation (docs.maple.finance) + maple-labs/address-registry	AUDIT DATE July 2026
VERIFIED ON-CHAIN 2026-07-15 · Ethereum block 25,537,989 · Base block 48,664,172 (via Etherscan v2)	REPORT VERSION v1.0
STATUS FINAL	

SECTION 03

Scope reviewed

Chains in scope

Ethereum · Base

Contracts in scope

CHAIN	CONTRACT	ADDRESS
ETH	daoMultisig (4-of-7)	0xd6d4Bcde6c816F17889f1Dd3000aF0261B03a196
ETH	GovernorTimelock	0x2eFFf88747EB5a3FF00d4d8d0f0800E306C0426b
ETH	MapleGlobals	0x804a6F5F667170F545Bf14e5DDB48C70B788390C
ETH	PoolPermissionManager	0xBe10aDcE8B6E3E02Db384E7FaDA5395DD113D8b3
ETH	MapleTreasury	0xa9466EaBd096449d650D5AEB0dD3dA6F52FD0B19
ETH	securityAdmin (3-of-6)	0x6b1A78C1943b03086F7Ee53360f9b0672bD60818
ETH	operationalAdmin (3-of-5)	0xCe1cE7c7F436DCc4E28Bc8bf86115514d3DC34E8
ETH	globalAdmin (2-of-3)	0x0D8b2C1F11c5f9cD51de6dB3b256C1e3b0800200
ETH	syrupUSDC PoolManager	0x7aD5fFa5fdF509E30186F4609c2f6269f4B6158F
ETH	syrupUSDT PoolManager	0x0cdA32E08B48bFDDbc7eE96B44b09cf286F9E21a
ETH	syrupUSDG PoolManager	0x6c48CD22086F3Db3F23E7cEeDD5c429D93FF3327
ETH	Institutional Secured-Lending PoolManager	0x9ceF7d1D390A4811bBa1BC40A53B40a506C33B19
ETH	SyrupToken	0x643C4E15d7d62Ad0aBeC4a9BD4b001aA3Ef52d66
ETH	SyrupOFT (LayerZero V2)	0x688AEe022AA544f150678B8E5720b6b96a9E9a2F
ETH	MapleCCIPReceiver (legacy)	0x02B6A75c5D1F430F0614dc5AC8aD5F9D35fbA2c4
BASE	MapleGlobals	0x7f3C3636208A18c7941BF051807db56864061465
BASE	Governor (Safe 3-of-5, no timelock)	0xD9481a47DFe8E5C35Eb809df25cdB5Bc2E24A3bE
BASE	MapleTreasury (Safe 1-of-1)	0x3A5ab01B4E142F41f54a861c984D19C866Ec1736
BASE	operationalAdmin (2-of-4)	0xa263B86eE90918Ce797E2Cf8d98c74E3Af50367f
BASE	CashMgmtUSDC PoolManager	0x7aA13F647691A709dc3360acAd7EB758179790ee
BASE	SyrupOFT (LayerZero V2)	0x688AEe022AA544f150678B8E5720b6b96a9E9a2F

Authorities audited

governor / GovernorTimelock, securityAdmin (pause), operationalAdmin, globalAdmin, daoMultisig, proxy / upgrade admins, pool delegates, LayerZero OFT owner + delegate, CCIP receiver, Aave / Sky strategy managers, Chainlink price feeds.

Out of scope

- 11 inactive / deprecated pools (AQRU, Maven11 ×4, Orthogonal, Cicada, Icebreaker, Laser, Lend+Long ×2, Blue Chip, High-Yield Corp, Cash-Mgmt USDC/USDT on ETH)
- Solana (non-EVM) deployment
- Smart-contract code correctness
- Credit / underwriting risk
- Off-chain key custody
- Signer identity attribution

SECTION 04

Security posture

WATCH — SOUND ETHEREUM CORE, CROSS-CHAIN GAPS

Maple's Ethereum governance is mature and timelocked with an independent top-level 4-of-7 Safe. The material gaps are cross-chain and operational: Base replicates the roles without a timelock or multi-party treasury, and the four Ethereum pool delegates are single keys. No critical or high on-chain theft vector was found — the findings are key-management and defense-in-depth.

SECTION 05

Severity definitions

SEVERITY	DEFINITION
CRITICAL	Active or imminent risk of total or substantial protocol compromise via the authority layer.
HIGH	Material risk of significant loss or operational compromise.
MEDIUM	Notable weakness with realistic exploit paths under specific conditions.
LOW	Hygiene issue or deprecated pattern. No immediate exploit path.
INFORMATIONAL	Observation or note. No risk classification.

SECTION 06

Status definitions

STATUS	MEANING
Open	Identified and verified on-chain; not yet remediated or formally accepted.
Acknowledged	The protocol team has recognised the finding; remediation is pending.
Remediated	Resolved on-chain and re-verified by Stabilitytics.
Risk-accepted	The protocol has formally accepted the risk with documented rationale.

SECTION 07

Findings summary

ID	TITLE	SEVERITY	PILLAR	STATUS
P1-001	Base upgrade authority executes with no timelock	MEDIUM	1	Open
P1-002	The four Ethereum pool delegates are single externally-owned keys	MEDIUM	1	Open
P2-001	Base protocol treasury is a 1-of-1 Safe	MEDIUM	2	Open
P1-003	Two Ethereum singletons upgrade outside the GovernorTimelock	MEDIUM	1	Open
P2-002	Low thresholds on powered roles; cross-chain pause is one shared team	LOW	2	Open
P3-001	LayerZero OFT delegate correctly set to a multisig on both chains (DVN quorum a residual check)	INFORMATIONAL	3	Open
P3-002	Legacy Chainlink CCIP receiver — confirm decommissioning	LOW	3	Open
P1-004	Governor can override oracle prices (timelocked on Ethereum only)	INFORMATIONAL	1	Open

SECTION 08

Roles & power distribution

Role inventory

CHAIN	CONTRACT	ROLE	HOLDER	TYPE	RISK
ETH	MapleGlobals	Proxy admin (EIP-1967)	0x2effff88747eb5a3ff00d4d8d0f0800e306c0426b	contract	–
ETH	MapleGlobals	Implementation (current)	0x9beabb1b6f3ad1ddb87b65148ba5eb6102334956	contract (logic)	–
ETH	MapleGlobals	governor()	0x2effff88747eb5a3ff00d4d8d0f0800e306c0426b	contract	–
ETH	MapleGlobals	pendingGovernor()	0x00000000000000000000000000000000	value	–
ETH	MapleGlobals	mapleTreasury()	0xa9466eabd096449d650d5aeb0dd3da6f52fd0b19	contract	–
ETH	MapleGlobals	securityAdmin()	0x6b1a78c1943b03086f7ee53360f9b0672bd60818	Safe 3-of-6	–
ETH	MapleGlobals	operationalAdmin()	0xce1ce7c7f436dcc4e28bc8bf86115514d3dc34e8	Safe 3-of-5	–
ETH	PoolPermissionManager	Proxy admin (EIP-1967)	0xd6d4bcde6c816f17889f1dd3000af0261b03a196	Safe 4-of-7	–
ETH	PoolPermissionManager	Implementation (current)	0xc3530358e54bc81efce4a2e12a898e996b091753	contract (logic)	–

CHAIN	CONTRACT	ROLE	HOLDER	TYPE	RISK
ETH	BorrowerActions	Proxy admin (EIP-1967)	0x6b1a78c1943 b03086f7ee5336 0f9b0672bd6081 8	Safe 3-of-6	–
ETH	BorrowerActions	Implementation (current)	0x78c5f240a115 0c3c2ebdbde559 d04a0418dfcff3	contract (logic)	–
ETH	PoolManagerFactory	mapleGlobals()	0x804a6f5f6671 70f545bf14e5d db48c70b788390 c	contract	–
ETH	PoolManagerFactory	defaultVersion()	400	value	–
ETH	FixedTermLoanFactory	mapleGlobals()	0x804a6f5f6671 70f545bf14e5d db48c70b788390 c	contract	–
ETH	FixedTermLoanFactory	defaultVersion()	601	value	–
ETH	FixedTermLoanManager	mapleGlobals()	0x804a6f5f6671 70f545bf14e5d db48c70b788390 c	contract	–
ETH	FixedTermLoanManager	defaultVersion()	301	value	–
ETH	OpenTermLoanFactory	mapleGlobals()	0x804a6f5f6671 70f545bf14e5d db48c70b788390 c	contract	–
ETH	OpenTermLoanFactory	defaultVersion()	201	value	–
ETH	OpenTermLoanManager	mapleGlobals()	0x804a6f5f6671 70f545bf14e5d db48c70b788390 c	contract	–
ETH	OpenTermLoanManager	defaultVersion()	100	value	–
ETH	WithdrawalManager	OpenFactory	0x804a6f5f6671 70f545bf14e5d db48c70b788390 c	contract	–
ETH	WithdrawalManager	defaultVersion()	200	value	–

CHAIN	CONTRACT	ROLE	HOLDER	TYPE	RISK
ETH	LiquidatorFactory	mapleGlobals()	0x804a6f5f667170f545bf14e5ddb48c70b788390c	contract	–
ETH	LiquidatorFactory	defaultVersion()	200	value	–
ETH	AaveStrategyFactory	mapleGlobals()	0x804a6f5f667170f545bf14e5ddb48c70b788390c	contract	–
ETH	AaveStrategyFactory	defaultVersion()	100	value	–
ETH	SkyStrategyFactory	mapleGlobals()	0x804a6f5f667170f545bf14e5ddb48c70b788390c	contract	–
ETH	SkyStrategyFactory	defaultVersion()	100	value	–
ETH	syrupUSDC PoolManager	Proxy admin (EIP-1967)	[object Object]	contract	–
ETH	syrupUSDC PoolManager	Implementation (current)	0xfe02be1ad28edfd8e3dd6f29c402b244c2a258b8	contract (logic)	–
ETH	syrupUSDC PoolManager	poolDelegate()	0xc1e18ffd8825ffb286d177ddebba345ec70b49f	EOA	MEDIUM
ETH	syrupUSDC PoolManager	pendingPoolDelegate()	0x00	value	MEDIUM
ETH	syrupUSDC FixedTermLoanManager	Proxy admin (EIP-1967)	[object Object]	contract	–
ETH	syrupUSDC FixedTermLoanManager	Implementation (current)	0x5b97c9dcce2693844b90cea40ba1fd15bf99eb01	contract (logic)	–
ETH	syrupUSDC OpenTermLoanManager	Proxy admin (EIP-1967)	[object Object]	contract	–

CHAIN	CONTRACT	ROLE	HOLDER	TYPE	RISK
ETH	syrupUSDC OpenTermLoanManager	Implementation (agent)	0xbad003da1e10 7f537ae2f687f5 fe7a7affe9b241	contract (logic)	–
ETH	syrupUSDC WithdrawalManager	Proxy admin (EIP-1967)	[object Object]	contract	–
ETH	syrupUSDC WithdrawalManager	Implementation (current)	0xf95e5722226 a1018d058cd757 b75f1d10289e96 7	contract (logic)	–
ETH	syrupUSDC AaveStrategy	Proxy admin (EIP-1967)	[object Object]	contract	–
ETH	syrupUSDC AaveStrategy	Implementation (current)	0xfc8f7f97165 d446b02cc95363 d2ca31154bbe9 f9	contract (logic)	–
ETH	syrupUSDC SkyStrategy	Proxy admin (EIP-1967)	[object Object]	contract	–
ETH	syrupUSDC SkyStrategy	Implementation (current)	0xbbee42621499 005ff0ddef947 bbdefbbbee7773 0	contract (logic)	–
ETH	syrupUSDT PoolManager	Proxy admin (EIP-1967)	[object Object]	contract	–
ETH	syrupUSDT PoolManager	Implementation (current)	0xfe02be1ad28 edfd8e3dd6f29 c402b244c2a258 b8	contract (logic)	–
ETH	syrupUSDT PoolManager	poolDelegate()	0x93aa06f8a7b b4da3eb0dd5a5 a38c01a7eb3550 1a	EOA	MEDIUM
ETH	syrupUSDT PoolManager	pendingPoolDelegate()	000000000000 00000000000000 00000000000000	value	MEDIUM
ETH	syrupUSDT FixedTermLoanManager	Proxy admin (EIP-1967)	[object Object]	contract	–

CHAIN	CONTRACT	ROLE	HOLDER	TYPE	RISK
ETH	syrupUSDT FixedTermLoanManager	Implementation (current)	0x5b97c9dcce26 93844b90cea40 ba1fd15bf99eb0 1	contract (logic)	-
ETH	syrupUSDT OpenTermLoanManager	Proxy admin (EIP-1967)	[object Object]	contract	-
ETH	syrupUSDT OpenTermLoanManager	Implementation (agent)	0xbad003da1e10 7f537ae2f687f5 fe7a7affe9b241	contract (logic)	-
ETH	syrupUSDT WithdrawalManager	Proxy admin (EIP-1967)	[object Object]	contract	-
ETH	syrupUSDT WithdrawalManager	Implementation (Queue)	0xf95e5722226 a1018d058cd757 b75f1d10289e96 7	contract (logic)	-
ETH	syrupUSDT AaveStrategy	Proxy admin (EIP-1967)	[object Object]	contract	-
ETH	syrupUSDT AaveStrategy	Implementation (current)	0xfc8f7f97165 d446b02cc95363 d2ca31154bbe9 f9	contract (logic)	-
ETH	syrupUSDG PoolManager	Proxy admin (EIP-1967)	[object Object]	contract	-
ETH	syrupUSDG PoolManager	Implementation (current)	0xfe02be1ad28 edfd8e3dd6f29 c402b244c2a258 b8	contract (logic)	-
ETH	syrupUSDG PoolManager	poolDelegate()	0x54e28bb2d530 ee10386dbca6e7 e84efac809292c	EOA	MEDIUM
ETH	syrupUSDG PoolManager	pendingPoolDelegate()	000000000000 00000000000000 00000000000000	value	MEDIUM
ETH	syrupUSDG OpenTermLoanManager	Proxy admin (EIP-1967)	[object Object]	contract	-
ETH	syrupUSDG OpenTermLoanManager	Implementation (agent)	0xbad003da1e10 7f537ae2f687f5 fe7a7affe9b241	contract (logic)	-

CHAIN	CONTRACT	ROLE	HOLDER	TYPE	RISK
ETH	syrupUSDG WithdrawalManager	Proxy admin (EIP-1967)	[object Object]	contract	–
ETH	syrupUSDG WithdrawalManager	Implementation (current)	0xf95e5722226 a1018d058cd757 b75f1d10289e96 7	contract (logic)	–
ETH	Institutional Secured- Lending PoolManager	Proxy admin (EIP-1967)	[object Object]	contract	–
ETH	Institutional Secured- Lending PoolManager	Implementation (current)	0xfe02be1ad28 edfd8e3dd6f29 c402b244c2a258 b8	contract (logic)	–
ETH	Institutional Secured- Lending PoolManager	poolDelegate()	0x8b5016578340 fc5011f5a35be3 02d665b88fede5	EOA	MEDIUM
ETH	Institutional Secured- Lending PoolManager	pendingPoolDelegate()	000000000000 000000000000000 000000000000000	value	MEDIUM
ETH	Institutional Secured- Lending FixedTermLoanManager	Proxy admin (EIP-1967)	[object Object]	contract	–
ETH	Institutional Secured- Lending FixedTermLoanManager	Implementation (current)	0x5b97c9dcce26 93844b90cea40 ba1fd15bf99eb0 1	contract (logic)	–
ETH	Institutional Secured- Lending OpenTermLoanManager	Proxy admin (EIP-1967)	[object Object]	contract	–
ETH	Institutional Secured- Lending OpenTermLoanManager	Implementation (current)	0xbad003da1e10 7f537ae2f687f5 fe7a7affe9b241	contract (logic)	–

CHAIN	CONTRACT	ROLE	HOLDER	TYPE	RISK
ETH	Institutional Secured-Lending WithdrawalManagerQueue	Proxy admin (EIP-1967)	[object Object]	contract	–
ETH	Institutional Secured-Lending WithdrawalManagerQueue	Implementation (current)	0xf95e5722226a1018d058cd757b75f1d10289e967	contract (logic)	–
ETH	Institutional Secured-Lending AaveStrategy	Proxy admin (EIP-1967)	[object Object]	contract	–
ETH	Institutional Secured-Lending AaveStrategy	Implementation (current)	0xfc8f7f97165d446b02cc95363d2ca31154bbe9f9	contract (logic)	–
ETH	Institutional Secured-Lending SkyStrategy	Proxy admin (EIP-1967)	[object Object]	contract	–
ETH	Institutional Secured-Lending SkyStrategy	Implementation (current)	0xbbee42621499005ff0ddef947bbdeffbbee77730	contract (logic)	–
ETH	SyrupToken	Proxy admin (EIP-1967)	[object Object]	contract	–
ETH	SyrupToken	Implementation (current)	0x6ed767ebcff51533e5181f7bf818f2b9bd767aec	contract (logic)	–
ETH	StSyrup	owner	0xd6d4bcde6c816f17889f1dd3000af0261b03a196	Safe 4-of-7	–
ETH	SyrupOFT	Proxy admin (EIP-1967)	0x47d23cfa96ce1ddee517266122e2602cb595679c	contract	–
ETH	SyrupOFT	Upgrade authority (ProxyAdmin owner)	0xce1ce7c7f436dcc4e28bc8bf86115514d3dc34e8	Safe 3-of-5	–

CHAIN	CONTRACT	ROLE	HOLDER	TYPE	RISK
ETH	SyrupOFT	Implementation (current)	0x08881c46f82325ce2e403097be40066fa8c326b2	contract (logic)	–
ETH	SyrupOFT	owner	0xce1ce7c7f436dcc4e28bc8bf86115514d3dc34e8	Safe 3-of-5	–
ETH	SyrupOFT	LZ delegate (EndpointV2)	0xce1ce7c7f436dcc4e28bc8bf86115514d3dc34e8	Safe 3-of-5	INFO
ETH	MapleCCIPReceiver	Proxy admin (EIP-1967)	[object Object]	contract	LOW
ETH	MapleCCIPReceiver	Implementation (current)	0x23cef2965db19f67a996371f9cb1a2f33d2b4821	contract (logic)	LOW
ETH	MapleCCIPReceiver	DEFAULT_ADMIN_ROLE	0xce1ce7c7f436dcc4e28bc8bf86115514d3dc34e8	Safe 3-of-5	LOW
ETH	Chainlink WETH/USD Oracle	owner	0x21f73d42eb58ba49ddb685dc29d3bf5c0f0373ca	Safe 4-of-9	–
ETH	Chainlink WBTC/USD Oracle	owner	0x21f73d42eb58ba49ddb685dc29d3bf5c0f0373ca	Safe 4-of-9	–
BASE	MapleGlobals	Proxy admin (EIP-1967)	0xd9481a47dfe8e5c35eb809df25cdb5bc2e24a3be	Safe 3-of-5	MEDIUM
BASE	MapleGlobals	Implementation (current)	0x5a64417823e8382a7e8957e4411873fe758e73a8	contract (logic)	–
BASE	MapleGlobals	governor()	0xd9481a47dfe8e5c35eb809df25cdb5bc2e24a3be	Safe 3-of-5	–
BASE	MapleGlobals	pendingGovernor()	0x00000000000000000000000000000000	value	–

CHAIN	CONTRACT	ROLE	HOLDER	TYPE	RISK
BASE	MapleGlobals	mapleTreasury()	0x3a5ab01b4e142f41f54a861c984d19c866ec1736	Safe 1-of-1	–
BASE	MapleGlobals	securityAdmin()	0x6150371231f783e97906af4861bc1ed11ce1c9ea	Safe 3-of-6	–
BASE	MapleGlobals	operationalAdmin()	0xa263b86ee90918ce797e2cf8d98c74e3af50367f	Safe 2-of-4	–
BASE	PoolPermissionManager	Proxy admin (EIP-1967)	0xd9481a47dfe8e5c35eb809df25cdb5bc2e24a3be	Safe 3-of-5	–
BASE	PoolPermissionManager	Implementation (current)	0xc3530358e54bc81efce4a2e12a898e996b091753	contract (logic)	–
BASE	PoolManagerFactory	mapleGlobals()	0x7f3c3636208a18c7941bf051807db56864061465	contract	–
BASE	PoolManagerFactory	defaultVersion()	300	value	–
BASE	FixedTermLoanFactory	mapleGlobals()	0x7f3c3636208a18c7941bf051807db56864061465	contract	–
BASE	FixedTermLoanFactory	defaultVersion()	502	value	–
BASE	FixedTermLoanManager	mapleGlobals()	0x7f3c3636208a18c7941bf051807db56864061465	contract	–
BASE	FixedTermLoanManager	defaultVersion()	200	value	–
BASE	OpenTermLoanFactory	mapleGlobals()	0x7f3c3636208a18c7941bf051807db56864061465	contract	–
BASE	OpenTermLoanFactory	defaultVersion()	101	value	–

CHAIN	CONTRACT	ROLE	HOLDER	TYPE	RISK
BASE	OpenTermLoanManagerFactory	mapleGlobals()	0x7f3c3636208a18c7941bf051807db56864061465	contract	–
BASE	OpenTermLoanManagerFactory	defaultVersion()	100	value	–
BASE	WithdrawalManagerOpenFactory	mapleGlobals()	0x7f3c3636208a18c7941bf051807db56864061465	contract	–
BASE	WithdrawalManagerOpenFactory	defaultVersion()	100	value	–
BASE	LiquidatorFactory	mapleGlobals()	0x7f3c3636208a18c7941bf051807db56864061465	contract	–
BASE	LiquidatorFactory	defaultVersion()	301	value	–
BASE	CashMgmtUSDC-BasePoolManager	Proxy admin (EIP-1967)	[object Object]	contract	–
BASE	CashMgmtUSDC-BasePoolManager	Implementation (current)	0x5b1d19ac5420ba8819aad6c0b98a41095e5c86c2	contract (logic)	–
BASE	CashMgmtUSDC-BasePoolManager	poolDelegate()	0xfcefe182bd1316d664e6f4073aa7cfb6b761bf b9	Safe 2-of-4	–
BASE	CashMgmtUSDC-BasePoolManager	pendingPoolDelegate()	00000000000000000000000000000000	value	–
BASE	CashMgmtUSDC-BaseFixedTermLoanManager	Proxy admin (EIP-1967)	[object Object]	contract	–
BASE	CashMgmtUSDC-BaseFixedTermLoanManager	Implementation (current)	0x7f6b190d3210bffaadbb0e83456b7c8030bc0f8b	contract (logic)	–
BASE	CashMgmtUSDC-BaseOpenTermLoanManager	Proxy admin (EIP-1967)	[object Object]	contract	–

CHAIN	CONTRACT	ROLE	HOLDER	TYPE	RISK
BASE	CashMgmtUSDC-Base OpenTermLoanManager	Implementation (current)	0xa6d0b2ca9f973c81ef94ccd8c62e4044f22972c1	contract (logic)	–
BASE	CashMgmtUSDC-Base WithdrawalManagerQueue	Proxy admin (EIP-1967)	[object object]	contract	–
BASE	CashMgmtUSDC-Base WithdrawalManagerQueue	Implementation (current)	0x899b57bbd8597aa2d1898476504f479c982c5c2c	contract (logic)	–
BASE	SyrupOFT	Proxy admin (EIP-1967)	0x47d23cfa96ce1dde517266122e2602cb595679c	contract	–
BASE	SyrupOFT	Upgrade authority (ProxyAdmin owner)	0xa263b86ee90918ce797e2cf8d98c74e3af50367f	Safe 2-of-4	–
BASE	SyrupOFT	Implementation (current)	0x08881c46f82325ce2e403097be40066fa8c326b2	contract (logic)	–
BASE	SyrupOFT	owner	0xa263b86ee90918ce797e2cf8d98c74e3af50367f	Safe 2-of-4	–
BASE	SyrupOFT	LZ delegate (EndpointV2)	0xa263b86ee90918ce797e2cf8d98c74e3af50367f	Safe 2-of-4	INFO

Cross-chain parity matrix

ROLE	ETH	BASE	PARITY
Proxy admin (EIP-1967) on MapleGlobals	contract	Safe 3-of-5 (3-of-5)	✗ Gap — differs across chains
governor() on MapleGlobals	contract	Safe 3-of-5 (3-of-5)	✗ Gap — differs across chains
pendingGovernor() on MapleGlobals	value	value	✓ Parity
mapleTreasury() on MapleGlobals	contract	Safe 1-of-1 (1-of-1)	✗ Gap — differs across chains

ROLE	ETH	BASE	PARITY
securityAdmin() on MapleGlobals	Safe 3-of-6 (3-of-6)	Safe 3-of-6 (3-of-6)	✓ Parity
operationalAdmin() on MapleGlobals	Safe 3-of-5 (3-of-5)	Safe 2-of-4 (2-of-4)	✗ Gap — differs across chains
Proxy admin (EIP-1967) on PoolPermissionManager	Safe 4-of-7 (4-of-7)	Safe 3-of-5 (3-of-5)	✗ Gap — differs across chains
mapleGlobals() on PoolManagerFactory	contract	contract	✓ Parity
defaultVersion() on PoolManagerFactory	value	value	✓ Parity
mapleGlobals() on FixedTermLoanFactoryV2	contract	contract	✓ Parity
defaultVersion() on FixedTermLoanFactoryV2	value	value	✓ Parity
mapleGlobals() on FixedTermLoanManagerFactory	contract	contract	✓ Parity
defaultVersion() on FixedTermLoanManagerFactory	value	value	✓ Parity
mapleGlobals() on OpenTermLoanFactory	contract	contract	✓ Parity
defaultVersion() on OpenTermLoanFactory	value	value	✓ Parity
mapleGlobals() on OpenTermLoanManagerFactory	contract	contract	✓ Parity
defaultVersion() on OpenTermLoanManagerFactory	value	value	✓ Parity
mapleGlobals() on WithdrawalManagerQueueFactory	contract	contract	✓ Parity
defaultVersion() on WithdrawalManagerQueueFactory	value	value	✓ Parity
mapleGlobals() on LiquidatorFactory	contract	contract	✓ Parity
defaultVersion() on LiquidatorFactory	value	value	✓ Parity
Proxy admin (EIP-1967) on SyrupOFT	contract	contract	✓ Parity
Upgrade authority (ProxyAdmin owner) on SyrupOFT	Safe 3-of-5 (3-of-5)	Safe 2-of-4 (2-of-4)	✗ Gap — differs across chains
owner on SyrupOFT	Safe 3-of-5 (3-of-5)	Safe 2-of-4 (2-of-4)	✗ Gap — differs across chains

ROLE	ETH	BASE	PARITY
LZ delegate (EndpointV2) on SyrupOFT	Safe 3-of-5 (3-of-5)	Safe 2-of-4 (2-of-4)	✗ Gap — differs across chains

Parity headline: Base upgrade authority (MapleGlobals governor/admin) is an untimelocked 3-of-5 Safe, whereas Ethereum routes the same authority through the GovernorTimelock (schedule->delay->execute). The asymmetry propagates to every factory-deployed contract on Base.

SECTION 09

Signer trust analysis

Per-signer profiles

Address	0xd6d4Bcde6c816F17889f1Dd3000aF0261B03a196
Type	Safe 4-of-7
In multisigs	Top-level governance / GovernorTimelock manager, PoolPermissionManager upgrade admin
Power weight	Root of Ethereum governance; manages the GovernorTimelock and upgrades PoolPermissionManager.
Attribution	Unattributed (no off-chain identity asserted)
Risk	LOW

Independent 7-signer set (no overlap with the operational admin Safes), 4-of-7 threshold — the strongest and best-separated Safe in the estate.

Address	0x6b1A78C1943b03086F7Ee53360f9b0672bD60818
Type	Safe 3-of-6
In multisigs	Emergency pause (Ethereum), BorrowerActions upgrade admin, recapitalizationClaimer
Power weight	Can pause every function in the protocol; upgrades BorrowerActions.
Attribution	Unattributed
Risk	MEDIUM

3-of-6 is reasonable, but it shares 5 of 6 signers with the Base securityAdmin — cross-chain pause is one team, not independent.

Address	0xCe1cE7c7F436DCc4E28Bc8bf86115514d3DC34E8
Type	Safe 3-of-5
In multisigs	Routine ops (Ethereum), SyrupOFT owner + LayerZero delegate (Ethereum)
Power weight	Owns the Syrup LayerZero OFT and is its endpoint delegate on Ethereum; routine ops.
Attribution	Unattributed

Risk

LOW

3-of-5 controlling the OFT configuration is adequate — healthier than the Base 2-of-4 equivalent.

Address 0x0D8b2C1F11c5f9cD51de6dB3b256C1e3b0800200

Type Safe 2-of-3

In multisigs Globals-level operational role (Ethereum)

Power weight Global operational admin.

Attribution Unattributed

Risk

MEDIUM

2-of-3 is the lowest threshold among the powered roles; its signers overlap both the security and operational Safes.

Address 0x6150371231f783e97906af4861Bc1eD11cE1c9Ea

Type Safe 3-of-6

In multisigs Emergency pause (Base)

Power weight Can pause the Base deployment.

Attribution Unattributed

Risk

MEDIUM

Same ~6-signer team as the Ethereum securityAdmin — no independent cross-chain incident response.

Address 0xa263B86eE90918Ce797E2Cf8d98c74E3Af50367f

Type Safe 2-of-4

In multisigs Routine ops (Base), SyrupOFT owner + LayerZero delegate (Base)

Power weight Owns the Base Syrup OFT and is its endpoint delegate; routine Base ops.

Attribution Unattributed

Risk

MEDIUM

2-of-4 controlling the Base OFT configuration is the weaker cross-chain link; recommend ≥ 3 -of-N.

Cross-multisig signer overlap

SIGNER	E:SECADMIN 3-OF-6	E:OPADMIN 3-OF-5	E:GLOBALADMIN 2-OF-3	B:SECADMIN 3-OF-6	B:OPADMIN 2-OF-4	NOTES
0x54cc... 3b74	✓	✗	✓	✓	✗	On three Safes — ETH security, ETH global, and Base security.
0x7371... 27af	✗	✓	✓	✗	✓	On three Safes — ETH ops, ETH global, and Base ops.
5 further signers	✓	✗	✗	✓	✗	The Ethereum and Base securityAdmin Safes share 5 of 6 signers — cross-chain pause is effectively one team. The 4-of-7 daoMultisig set is independent of all of the above.

SECTION 10

Third-party integrations

Integration inventory

#	INTEGRATION	CHAIN	INSTANCE	CONFIGURATION	RISK
1	LayerZero V2 OFT (SYRUP)	ETH	SyrupOFT 0x688AEe... 9a2F (same address both chains)	owner + endpoint delegate = operationalAdmin Safe (ETH 3-of-5, Base 2-of-4), confirmed via LZCheck; type OFTAdapter (sender v1 / receiver v2); no warnings. DVN quorum not enumerated this pass.	INFO
2	Chainlink CCIP receiver (legacy)	ETH	MapleCCIPReceiver 0x02B6...a2c4	router/owner unresolved this pass; superseded by the LayerZero OFT — confirm decommissioned.	LOW
3	Aave v3 yield strategy	ETH	AaveStrategy on syrupUSDC / syrupUSD / Institutional	pools deploy idle liquidity into Aave; strategy management is Governor-gated.	LOW
4	Sky (USDS) yield strategy	ETH	SkyStrategy on syrupUSDC / Institutional	idle liquidity into Sky/USDS savings; Governor-gated.	LOW
5	Chainlink price feeds	ETH	USDC/USD, WETH/USD, WBTC/USD	canonical Chainlink aggregators; Globals exposes setPriceOracle + setManualOverridePrice (timelocked on ETH, not on Base).	LOW
6	Upgradeable proxy model	ETH	MapleProxyFactory + NonTransparentProxy (all factory-deployed contracts, Globals, PPM)	upgrade authority = Globals governor: GovernorTimelock on ETH; 3-of-5 Safe with no timelock on Base.	MEDIUM

LayerZero SYRUP OFT — owner/delegate confirmed (LZCheck); DVN quorum a residual read

PATHWAY	OAPP OWNER	LZ DELEGATE	REQ DVN	OPTIONAL	LIBRARY
ETH → Base	Safe 3-of-5	Safe 3-of-5	not read	—	ULN v2
Base → ETH	Safe 2-of-4	Safe 2-of-4	not read	—	ULN v2

Default-vs-customized

INTEGRATION	DEFAULTS RETAINED?	STATUS	RISK IF DEFAULTS
LayerZero SYRUP OFT (ETH ↔ Base)	DVN quorum not enumerated (LZCheck delegate-focused)	Delegate = multisig on both chains (confirmed) — avoids the Kelp unset- delegate mode	INFO

SECTION 11

Audit findings

MEDIUM (4)

P1-001 Base upgrade authority executes with no timelock**MEDIUM**

Location Base — MapleGlobals 0x7f3C...1465 · admin() = governor() → 0xD948...A3bE (Gnosis Safe 3-of-5)

Status accepted

DESCRIPTION

On Ethereum, MapleGlobals (0x804a...390C) reports admin() and governor() = 0x2eFF...426b, an on-chain GovernorTimelock; all MapleProxyFactory version registrations and Governor-permissioned parameter changes execute through its schedule → delay → execute window. On Base, the equivalent MapleGlobals (0x7f3C...1465) reports admin() and governor() = 0xD948...A3bE, which eth_getCode identifies as a GnosisSafeProxy with an on-chain threshold of 3-of-5 — a plain multisig with no timelock in the path. Because every Base factory reads this same Globals as its upgrade authority, the entire Base upgradeable surface inherits the no-timelock property. On Ethereum the delay is enforced as per-function timelock windows configured in Globals (setTimelockWindow), not a single global scalar; on Base there is no timelock contract in the path at all.

IMPACT

On Base, any Governor-permissioned action — registering a new implementation version and upgrading pools/managers, setPriceOracle / setManualOverridePrice, setProtocolPause, setValidBorrower, fee-rate changes — takes effect the instant the 3-of-5 executes, with no scheduling delay and no window for LPs to withdraw or monitors to react. A compromise or collusion of the 3-of-5 yields immediate, irreversible control of the Base deployment. Drift Protocol ran a 2-of-5 multisig with zero timelock and lost ~\$285M when two signatures were obtained; the absence of a timelock turned a signer compromise into an instant, uncontestable drain.

REPRODUCTION / EVIDENCE

```
Base eth_call MapleGlobals(0x7f3C3636208A18c7941BF051807db56864061465): admin() = governor() = 0xD9481a47DFe8E5C35Eb809df25cdB5Bc2E24A3bE; eth_getCode = GnosisSafeProxy, getThreshold() = 3, getOwners().length = 5. Ethereum eth_call MapleGlobals(0x804a...390C): admin() = governor() = 0x2eFFf88747EB5a3FF00d4d8d0f0800E306C0426b (contractName GovernorTimelock, verified). Base block 48,664,172; Ethereum block 25,537,989.
```

RECOMMENDATION

- Deploy a GovernorTimelock on Base mirroring Ethereum and transfer MapleGlobals admin()/governor() to it, so Governor-permissioned actions and factory upgrades on Base pass through a schedule → delay → execute window.
- Until then, publish the intended Base timelock windows and treat the 3-of-5 as a hot governance key with heightened monitoring.
- Verify after change: MapleGlobals.governor() on Base resolves to the timelock contract, not a Safe/EOA.

REFERENCES

[Drift Protocol — 2-of-5 multisig, no timelock \(~\\$285M\)](#)

P1-002

The four Ethereum pool delegates are single externally-owned keys

MEDIUM

Location

Ethereum — poolDelegate() on syrupUSDC / syrupUSDT / syrupUSDG / Institutional Secured-Lending PoolManagers

Status

accepted

DESCRIPTION

Each active pool is administered by a Pool Delegate that configures pool parameters, manages Aave/Sky strategies, and funds loans from pool liquidity. On all four Ethereum pools the poolDelegate() resolves to an externally-owned account (eth_getCode = 0x): syrupUSDC 0x7aD5...158F → 0xc1e1...b49f; syrupUSDT 0x0cdA...E21a → 0x93aa...501a; syrupUSDG 0x6c48...3327 → 0x54e2...292c; Institutional Secured-Lending 0x9ceF...3B19 → 0x8b50...ede5. The Base Cash-Management pool, by contrast, uses a 2-of-4 Safe delegate — the multisig pattern is available in-protocol.

IMPACT

A Pool Delegate key is a single point of compromise for the highest-TVL pools; a stolen key can reconfigure strategies and originate loans against pool liquidity. The drain is bounded by a Governor-gated control — borrowers must be validated via setValidBorrower (timelocked on Ethereum) — so arbitrary-address theft is not directly possible; the realistic exposure is collusion with an already-validated borrower plus strategy/parameter manipulation. This is key-management hygiene on the protocol's largest pools: Resolv Labs lost ~\$25M when a single privileged EOA, held for ~2 years, was compromised via a contractor credential.

REPRODUCTION / EVIDENCE

```
eth_call poolDelegate() on each PoolManager returns the four EOAs above; eth_getCode on each = 0x. Counter-example: Base CashMgmtUSDC PoolManager 0x7aA1...90ee poolDelegate() = 0xfcef...bfb9 (Gnosis Safe 2-of-4). Ethereum block 25,537,989.
```

RECOMMENDATION

- Migrate each Ethereum Pool Delegate to a ≥ 3 -of-N multisig, matching the Base Cash-Management pool's Safe delegate.
- Interim: enforce hardware/MPC custody of delegate keys and monitor delegate actions (loan funding, strategy changes).
- Verify after change: poolDelegate() on each PoolManager resolves to a Safe with threshold ≥ 3 .

REFERENCES

Resolv Labs — single privileged EOA (~\$25M)

P2-001 Base protocol treasury is a 1-of-1 Safe**MEDIUM**

Location Base — `MapleGlobals.mapleTreasury()` → `0x3A5a...1736` (Gnosis Safe 1-of-1)

Status accepted

DESCRIPTION

On Base, `MapleGlobals.mapleTreasury()` resolves to `0x3A5a...1736`, a Gnosis Safe with a threshold of 1 of 1 owner. Accrued protocol fees on Base route to this address. A 1-of-1 Safe provides no multi-party control — it is functionally a single externally-owned key with a Safe wrapper.

IMPACT

A single signer can move all protocol-fee balances held by the Base treasury, and a single key compromise loses those funds with no second approver. Scope is limited to Base fee balances (not pool principal), which bounds the severity, but the single-key structure is below the standard expected of treasury custody — the same single-key class as the Resolv compromise.

REPRODUCTION / EVIDENCE

```
Base eth_call MapleGlobals.mapleTreasury() = 0x3A5ab01B4E142F41f54a861c984D19C866Ec1736;  
eth_getCode = GnosisSafeProxy; getThreshold() = 1, getOwners().length = 1. Base block  
48,664,172.
```

RECOMMENDATION

- Raise the Base treasury Safe to ≥ 2 -of-3 with independent signers.
- Verify via `getThreshold()  $\geq 2$` and `getOwners()` on `0x3A5a...1736`.

REFERENCES

Resolv Labs — [single privileged EOA \(~\\$25M\)](#)

P1-003 Two Ethereum singletons upgrade outside the GovernorTimelock MEDIUM

Location	Ethereum — PoolPermissionManager 0xBe10...D8b3 (proxy admin = daoMultisig 4-of-7) · BorrowerActions 0x70Eb...9E20 (proxy admin = securityAdmin 3-of-6)
-----------------	--

Status	accepted
---------------	----------

DESCRIPTION

Most Maple contracts upgrade through MapleProxyFactory under GovernorTimelock control. Two Ethereum singletons, however, are NonTransparentProxy instances whose EIP-1967 admin slot is a multisig that can upgrade them directly, bypassing the timelock: PoolPermissionManager (0xBe10...D8b3) admin = daoMultisig 0xd6d4...a196 (Safe 4-of-7); BorrowerActions (0x70Eb...9E20) admin = securityAdmin 0x6b1A...0818 (Safe 3-of-6). By contrast MapleGlobals' own proxy admin is the GovernorTimelock. PoolPermissionManager governs lender allowlists and permission levels for every pool.

IMPACT

These multisigs can replace the logic of the lender-permissioning contract (and BorrowerActions) with immediate effect, with none of the schedule → delay → execute buffer that protects the factory-governed surface. The Safes are robust (4-of-7, 3-of-6), so this is defense-in-depth rather than an acute vector — but it leaves the contract that decides who may lend and withdraw outside the timelock guarantee a reader would assume applies protocol-wide. Drift's no-timelock admin authority is what let an obtained signature set take effect instantly and irreversibly.

REPRODUCTION / EVIDENCE

```
eth_call on the EIP-1967 admin slot (0xb531...6103) of PoolPermissionManager 0xBe10...D8b3 = 0xd6d4...a196 (Safe 4-of-7); of BorrowerActions 0x70Eb...9E20 = 0x6b1A...0818 (Safe 3-of-6). MapleGlobals admin slot = 0x2eFF...426b (GovernorTimelock). Ethereum block 25,537,989.
```

RECOMMENDATION

- Route the upgrade admin of PoolPermissionManager and BorrowerActions through the GovernorTimelock, matching the factory-governed surface.
- If the direct-multisig path is intentional (e.g., emergency permissioning), document the exception and its compensating monitoring.
- Verify: the EIP-1967 admin of these proxies resolves to the timelock.

REFERENCES

[Drift Protocol — no-timelock admin authority \(~\\$285M\)](#)

LOW (2)

P2-002

Low thresholds on powered roles; cross-chain pause is one shared team

LOW

Location

Ethereum globalAdmin 0x0D8b...0200 (2-of-3) · Base operationalAdmin 0xa263...367f (2-of-4) · securityAdmin ETH 0x6b1A...0818 / Base 0x6150...c9Ea (both 3-of-6, 5 shared signers)

Status

accepted

DESCRIPTION

Across the six governance Safes (22 distinct signers), two carry low thresholds relative to their power: the Ethereum globalAdmin is 2-of-3, and the Base operationalAdmin is 2-of-4 — and the latter is the owner and LayerZero delegate of the Base SyrupOFT. The Ethereum and Base securityAdmin Safes (both 3-of-6) share five of six signers, so emergency-pause authority on both chains is effectively one team. The daoMultisig (4-of-7) has an independent signer set.

IMPACT

A 2-of-N role lowers the collusion/compromise bar for privileged actions; the Base operationalAdmin's 2-of-4 controls the cross-chain OFT configuration. The shared securityAdmin signer set means a compromise of that group affects pause capability on both chains simultaneously — cross-chain incident response is not independent. Drift's 2-of-5 low threshold was the structural weakness that made two obtained signatures sufficient.

REPRODUCTION / EVIDENCE

```
Safe getThreshold()/getOwners(): globalAdmin 0x0D8b...0200 = 2-of-3; Base operationalAdmin 0xa263...367f = 2-of-4 (also SyrupOFT owner + LZ delegate on Base); securityAdmin ETH 0x6b1A...0818 and Base 0x6150...c9Ea both 3-of-6 with 5 common owners. Ethereum block 25,537,989; Base block 48,664,172. LZCheck confirms signer 0x7371Da5AC817C05547da65a84EACd72D653027AF sits on both the Ethereum operationalAdmin (3-of-5) and Base operationalAdmin (2-of-4) Safes — cross-chain operational control also shares a signer.
```

RECOMMENDATION

- Raise powered-role thresholds to ≥ 3 -of-N (globalAdmin, Base operationalAdmin).
- Consider partially independent signer sets for securityAdmin per chain so cross-chain pause is not single-team.
- Verify via getThreshold()/getOwners().

REFERENCES

[Drift Protocol — low-threshold multisig \(~\\$285M\)](#)

P3-002 Legacy Chainlink CCIP receiver — confirm decommissioning

LOW

Location Ethereum — MapleCCIPReceiver 0x02B6...a2c4**Status** accepted**DESCRIPTION**

The registry lists a MapleCCIPReceiver (0x02B6...a2c4) from an earlier Chainlink CCIP-based cross-chain design. SYRUP's active cross-chain transport is now the LayerZero OFT (P3-001). On this pass the receiver's `getRouter()` and `owner()` calls returned null (proxy/implementation or paused), so its current authority could not be characterised from the standard getters.

IMPACT

A legacy cross-chain receiver that still holds mint, allowlist, or message-authorisation rights but is no longer actively monitored is an orphaned attack surface — the class of risk behind bridge-glue incidents such as Hyperbridge, where a forged message minted 1 billion bridged DOT. If the receiver has been fully decommissioned (no router, no authority), the risk is nil; this needs explicit confirmation.

REPRODUCTION / EVIDENCE

```
eth_call getRouter() and owner() on 0x02B6A75c5D1F430F0614dc5AC8aD5F9D35fbA2c4 returned null at
Ethereum block 25,537,989 (the contract is a proxy; implementation/selector unresolved).
Registry classifies it as MapleCCIPReceiver. Targeted re-read (block 25,538,213): the contract
is an ERC1967Proxy with implementation 0x23CEF2965Db19f67A996371F9Cb1A2F33D2b4821; ten candidate
accessors (getRouter/router/i_ccipRouter/ccipRouter/s_router/owner/globals/syrup/token) all
returned null, so its live router and authority must be read from the verified implementation
ABI before decommissioning is assumed.
```

RECOMMENDATION

- Read the receiver's router and any mint/allowlist authority via its verified implementation ABI; if superseded by the OFT, revoke its permissions and document decommissioning.
- If retained, bring it into monitored scope alongside the LayerZero OFT.
- Verify no privileged role on the receiver remains held by a live key.

REFERENCES

[Hyperbridge — forged bridge message, 1B DOT minted](#)

INFORMATIONAL (2)

P3-001

LayerZero OFT delegate correctly set to a multisig on both chains (DVN quorum a residual check)

INFORMATIONAL

Location Ethereum & Base — SyrupOFT 0x688A...9a2F · EndpointV2 0x1a44...728c

Status accepted

DESCRIPTION

SYRUP bridges between Ethereum and Base as a LayerZero V2 OFTAdapter (0x688A...9a2F on both chains, endpoint 0x1a44...728c, eids 30101/30184). An LZCheck verification confirms the OApp owner and the endpoint delegate are the same operationalAdmin Safe on each chain — a multisig, not the unset / single-key delegate that enabled the Kelp DAO loss. The delegate is the role that controls the message-verification configuration (DVN set, libraries); its being a multisig on both chains is the healthy configuration. The DVN quorum itself is not surfaced by this pass (LZCheck focuses on the delegate role, the post-Kelp failure mode) and remains a residual spot-check.

IMPACT

The delegate controls the DVN/library stack that verifies cross-chain messages before SYRUP is released. Here it is a multisig on both chains (ETH 3-of-5, Base 2-of-4), which avoids the Kelp DAO failure mode (~\$290M) where a mis-set delegate/1-of-1 DVN let a forged packet through. Residual, lower-priority item: the required-DVN quorum on each pathway was not enumerated in this pass; given LayerZero's post-Kelp default hardening it is defense-in-depth rather than an open exposure.

REPRODUCTION / EVIDENCE

```
LZCheck POST /verify - chainId 1: owner = delegate = 0xCe1cE7c7F436DcC4E28Bc8bf86115514d3DC34E8
(Safe 1.3.0, 3-of-5; owners incl. 0x7371Da...27AF). chainId 8453: owner = delegate =
0xa263B86eE90918Ce797E2Cf8d98c74E3Af50367f (Safe 1.3.0, 2-of-4; owners incl. 0x7371Da...27AF).
type OFTAdapter (sender v1 / receiver v2); warnings: none. Endpoint 0x1a44...728c. Verified
2026-07-15 (Ethereum block 25,537,989 · Base block 48,664,172). DVN quorum (ULN getConfig,
configType 2) not enumerated in this pass.
```

RECOMMENDATION

- Keep the OFT delegate as the operationalAdmin multisig on both chains; periodically re-verify it is never left unset or reassigned to an EOA (the Kelp failure mode).
- As defense-in-depth, read the ULN config (Endpoint getConfig, configType 2) per pathway and confirm ≥ 2 required DVNs including a non-LayerZero-Labs DVN.
- Raise the Base operationalAdmin from 2-of-4 toward 3-of-N given it is also the OFT delegate (see P2-002).

REFERENCES

[Kelp DAO / LayerZero — 1-of-1 default DVN \(~\\$290M\)](#)

P1-004

Governor can override oracle prices (timelocked on Ethereum only)

INFORMATIONAL

Location	Ethereum & Base — MapleGlobals setPriceOracle / setManualOverridePrice
-----------------	--

Status	accepted
---------------	----------

DESCRIPTION

MapleGlobals exposes the Governor-permissioned functions setPriceOracle and setManualOverridePrice, letting governance substitute a collateral price feed or set a manual override price used in liquidations and valuations. In-scope price feeds are Chainlink aggregators (USDC/USD 0x5DC5...64E7, WETH/USD 0x5f4e...8419, WBTC/USD 0xF403...E88C). On Ethereum these calls pass through the GovernorTimelock; on Base they do not (see P1-001).

IMPACT

This is a legitimate administrative capability, but it concentrates a market-integrity lever — the price used to value collateral and trigger liquidations — in governance, and on Base it is exercisable with no timelock. An attacker-controlled or mis-set price is the mechanism behind numerous DeFi losses (e.g., Drift's permissive market fed by an attacker-controlled oracle). Informational: it is Governor-gated and, on Ethereum, timelocked.

REPRODUCTION / EVIDENCE

MapleGlobals Governor-permissioned function set includes setPriceOracle and setManualOverridePrice (Maple admin docs). Price feeds in scope: 0x5DC5...64E7, 0x5f4e...8419, 0xF403...E88C. Timelock applies on Ethereum (governor = GovernorTimelock) but not on Base (governor = 3-of-5 Safe). Ethereum block 25,537,989; Base block 48,664,172.

RECOMMENDATION

- Constrain manual price overrides behind the timelock on both chains and bound the permitted deviation.
- Emit monitored events on oracle changes and publish the override policy.

REFERENCES

[Drift Protocol — attacker-controlled oracle feed \(~\\$285M\)](#)

SECTION 12

Centralisation & power concentration

Authority over the Maple estate is layered and, on Ethereum, genuinely well-structured. Upgrades to factory-deployed contracts and Governor-permissioned parameter changes are registered and executed through the on-chain GovernorTimelock (0x2eFF...426b), which is in turn managed by governance multisigs; the top-level daoMultisig is a 4-of-7 Safe whose signer set is independent of the operational admin Safes. Emergency pause is a 3-of-6 securityAdmin and routine operations a 3-of-5 operationalAdmin. This is a mature configuration.

The concentration risk is cross-chain asymmetry. On Base the same logical roles exist, but the safeguards do not: MapleGlobals' governor and proxy admin are a single 3-of-5 Safe with no timelock, so every Base factory and pool can be upgraded, re-oracled, or unpaused instantly; the Base treasury is a 1-of-1 Safe. A reader who assumes the Ethereum timelock protects the whole protocol would be mistaken for Base.

One level below governance, day-to-day pool authority on Ethereum rests on single externally-owned keys — the four Pool Delegates — whose custody is off-chain and load-bearing. Maple's design constrains what a delegate can do (borrowers are Governor-validated), so this is an operational key-management surface rather than a direct theft vector, but it is the practical attack surface and has not kept pace with the multisig discipline applied at the governance layer (the Base Cash-Management pool already uses a 2-of-4 Safe delegate). At the token layer, SYRUP issuance is governed through MapleGlobals (SyrupToken.globals() = 0x804a...390C) and the RecapitalizationModule rather than a standalone owner key — a positive, and a contrast with deployments whose mint authority reduces to a single EOA.

SECTION 13

Remediation roadmap

PRIORITY	FINDING	RECOMMENDATION	EFFORT	OWNER
1 (immediate)	P1-002	Migrate the four Ethereum Pool Delegates onto ≥ 3 -of-N multisigs (matching the Base pool)	1-2 days	Protocol team
1 (immediate)	P2-001	Raise the Base treasury Safe from 1-of-1 to ≥ 2 -of-3 independent signers	1 day	Protocol team
2 (this week)	P1-001	Deploy a GovernorTimelock on Base; route MapleGlobals governor/admin through it	3-5 days	Protocol team
2 (this week)	P3-001	Run LZCheck on the ETH↔Base SyrupOFT pathways; confirm ≥ 2 required DVNs	1 day	Stabilitytics + Protocol
2 (this week)	P3-002	Confirm the legacy CCIP receiver is decommissioned / holds no live authority	1 day	Protocol team
3 (this month)	P1-003	Bring PoolPermissionManager + BorrowerActions upgrades under the GovernorTimelock	2-3 days	Protocol team
3 (this month)	P2-002	Raise globalAdmin (2-of-3) and Base operationalAdmin (2-of-4) thresholds; consider independent cross-chain securityAdmin sets	1 day	Protocol team
4 (review)	P1-004	Constrain governor oracle overrides behind the timelock on both chains; bound deviation	discussion	Protocol team

SECTION 14

Conclusion

Maple Finance presents a mature governance posture on Ethereum wrapped around two gaps: a Base deployment that replicates the roles without the timelock or multi-party safeguards, and an operational key layer (pool delegates, Base treasury) that sits on single keys. None of the findings is a critical on-chain vulnerability, and each has a concrete, low-effort remediation.

In priority order: (1) migrate the four Ethereum Pool Delegates and the Base 1-of-1 treasury onto multisigs; (2) deploy a GovernorTimelock on Base and route the Globals governor and proxy admin through it; (3) bring PoolPermissionManager and BorrowerActions upgrades under the Ethereum timelock and raise the 2-of-N thresholds; (4) run LZCheck on the Syrup OFT pathways and confirm the legacy CCIP receiver is decommissioned. The LayerZero DVN and CCIP items should be closed before this report is treated as complete on Pillar 3.

SECTION 15

Methodology

Stabilitytics performed a Live Infrastructure Audit (LIA) across Pillars 1 (roles & power distribution), 2 (signer trust structure) and 3 (integration configuration) against live on-chain state on Ethereum and Base — not source code. Every privileged role and authority was enumerated from on-chain reads: the Globals governor / admin / treasury / security / operational getters, per-pool poolDelegate, per-factory globals and defaultVersion, proxy admin and implementation slots, and Safe owners and threshold for each governance multisig.

Upgrade authority was read from EIP-1967 storage slots and from Maple's factory model (MapleProxyFactory version registration under the Globals governor). Cross-chain integration was characterised from the Syrup LayerZero OFT owner and EndpointV2 delegate on both chains; the DVN / ULN verification stack is enumerated separately via LZCheck and is noted where pending. Signer overlap was computed across all six governance Safes.

AI and scanners accelerated enumeration; every finding and severity call was verified by a human Stabilitytics engineer, and every material finding was independently peer-reviewed before transmission. The tool reports facts; severity and recommendations are human-owned.

All reads were verified on Ethereum mainnet (block 25,537,989) and Base (block 48,664,172) on 2026-07-15. Three getter values — the Ethereum GovernorTimelock's delay parameter, the CCIP receiver's router / owner, and the Syrup token's mint-owner accessor — did not resolve on this pass and are noted as pending targeted re-reads; they refine findings P1-004 / P3-001 / P3-002 but do not affect the Pillar 1 role map.

SECTION 16

Disclaimer & scope limits

Findings reflect on-chain state at the moment of verification (2026-07-15). Configurations may change after delivery.

This is an unsolicited public report. Stabilytics was not engaged or compensated by Maple Finance. All findings are based on publicly available on-chain data and public documentation at docs.maple.finance.

Stabilytics did not perform smart-contract code review, credit / underwriting assessment, off-chain key-custody assessment, or signer identity attribution.

Scope was the active deployment: the five active pools (syrupUSDC / USDT / USDG, Maple Institutional Secured-Lending, and the Base Cash-Management pool), shared core, factories and integrations. The 11 inactive / deprecated pools and the non-EVM (Solana) deployment were out of scope.

The Syrup LayerZero DVN configuration and the legacy CCIP receiver were not fully characterised in this pass (Pillar 3 items P3-001 / P3-002) and should be confirmed before Pillar 3 is treated as complete.

SECTION 17

About Stabilytics

Stabilytics audits the **live deployment** of Web3 protocols — the roles, signers, and third-party integrations that determine who controls a protocol and what happens if that control is compromised. This is the layer between a smart-contract audit (does the code do what it says?) and an OPSEC review (do the people follow safe practices?) — a blind spot that has cost protocols hundreds of millions of dollars.

Engagements are **human-authored and peer-reviewed**; tooling accelerates enumeration but every finding and severity call is owned by a human engineer. Web: stabilytics.fi · Contact: ops@stabilytics.fi.



Issued by Stabilytics. Human-authored by a Stabilytics engineer. Every Critical and High finding independently peer-reviewed by a second engineer before transmission. Reports are issued under the Stabilytics name; reviewer identities are an internal coordination matter.

Questions: ops@stabilytics.fi · Web: stabilytics.fi