MASTER PROTOCOL REVIEW REPORT

Overall Structural Integrity: REQUIRES REVISION

Critical Findings Summary: - None.

Major Findings Summary: - contracts/core/Vault.sol:160 Emergency activation moves all assets to emergencyCustodian and permanently blocks deposit/withdraw, but no on-chain user redemption path exists afterward; this creates a hard custody/funds-availability risk. - contracts/core/Vault.sol:148 managedAssets() treats emergencyCustodiedAssets as continuously available assets even though custody is off-contract and unverifiable after transfer, so solvency can be overstated. - contracts/core/VaultFactory.sol:45 Any caller can instantiate vaults with arbitrary custodian addresses; deterministic deployment remains correct, but operational safety depends on strict off-chain allowlisting/discovery controls.

Invariant Status: - Liability Conservation: PASS - Solvency: FAIL - No-liability-without-custody-delta: PASS - Emergency Neutrality: FAIL

Deterministic Deployment Integrity: - CREATE2 Model: VALID - Salt Model: VALID - Registry Model: VALID

Storage Stability: - Layout Frozen: YES - Clone Safe: YES

Security Posture: - Funds at Risk: YES - Privilege Escalation Risk: NONE - Reentrancy Risk: MITIGATED

Gas Profile: - Acceptable for production: YES - Optimization recommended: YES

Final Verdict: REQUIRES ARCHITECTURAL REVISION

Review Completion Status: FULL REVIEW COMPLETED

End of Report. SPEC COMPLIANCE REPORT

Specification Version: v1.0 (docs/spec_v1.md, Git Commit: 6964689)

Code Baseline: Commit 6964689 + working tree modifications present

Overall Compliance Status: PARTIALLY COMPLIANT

Compliance Summary: - Total requirements: 24 - Compliant: 23 - Partial: 1 - Non-compliant: 0 - Not applicable: 0 - Silent features detected: 4 - Spec drift risk: LOW

Critical Misalignments: - None.

High-Risk Misalignments: - None.

Compliance Matrix:

[R1] - Spec Clause: Deterministic Deployment Model: “Factory deploys vault clones via CREATE2.” - Code Reference: contracts/core/VaultFactory.sol:76, contracts/core/VaultFactory.sol:65 - Expected Behavior: Deterministic CREATE2 clone deployment from factory. - Observed Behavior: Uses Clones.cloneDeterministic and predictDeterministicAddress. - Status: COMPLIANT - Deviation Type: Functional - Severity: INFO - Impact: Deterministic deployment model implemented. - Remediation Direction: None.

[R2] - Spec Clause: Deterministic identity derived from domain-separated salt inputs. - Code Reference: contracts/core/VaultFactory.sol:54, contracts/libraries/DeterministicSalt.sol:5-22 - Expected Behavior: Identity salt is domain-separated and canonical. - Observed Behavior: Salt derived through DeterministicSalt.deriveSalt with domain constant and canonical fields. - Status: COMPLIANT - Deviation Type: Functional - Severity: INFO - Impact: Identity derivation aligned with spec. - Remediation Direction: None.

[R3] - Spec Clause: Registry bindings vaultBySalt[salt] -> vault. - Code Reference: contracts/core/VaultFactory.sol:21, contracts/core/VaultFactory.sol:85 - Expected Behavior: Canonical salt-to-vault mapping populated on create. - Observed Behavior: vaultBySalt[finalSalt] = vault after successful init. - Status: COMPLIANT - Deviation Type: Functional - Severity: INFO - Impact: Canonical lookup available. - Remediation Direction: None.

[R4] - Spec Clause: Registry bindings isVault[vault] -> true. - Code Reference: contracts/core/VaultFactory.sol:22, contracts/core/VaultFactory.sol:86 - Expected Behavior: Registry marks deployed vaults as valid. - Observed Behavior: isVault[vault] = true on creation. - Status: COMPLIANT - Deviation Type: Functional - Severity: INFO - Impact: Trust-boundary checks supported. - Remediation Direction: None.

[R5] - Spec Clause: Canonical salt equation with (SALT_DOMAIN, chainid, factory, underlying, admin, userSalt). - Code Reference: contracts/libraries/DeterministicSalt.sol:13-21 - Expected Behavior: Exact canonical field order and contents. - Observed Behavior: Exact order and field set implemented. - Status: COMPLIANT - Deviation Type: Functional - Severity: INFO - Impact: Address determinism and cross-chain separation preserved. - Remediation Direction: None.

[R6] - Spec Clause: SALT_DOMAIN = keccak256("DETERMINISTIC_VAULT_FACTORY_V1"). - Code Reference: contracts/libraries/DeterministicSalt.sol:5 - Expected Behavior: Exact domain constant. - Observed Behavior: Exact constant string and hashing function used. - Status: COMPLIANT - Deviation Type: Functional - Severity: INFO - Impact: Domain separation aligned. - Remediation Direction: None.

[R7] - Spec Clause: I1 Liability Conservation totalAssets == Σ balances[user]. - Code Reference: contracts/core/Vault.sol:111-113, contracts/core/Vault.sol:135-137, contracts/core/Vault.sol:160-190 - Expected Behavior: Liability state changes only by equal user-balance deltas. - Observed Behavior: Deposit/withdraw mutate balances and totalAssets by identical deltas; emergency leaves liabilities unchanged. - Status: COMPLIANT - Deviation Type: Invariant - Severity: INFO - Impact: Liability conservation maintained by transitions in scope. - Remediation Direction: None.

[R8] - Spec Clause: I2 Solvency managedAssets >= totalAssets. - Code Reference: contracts/core/Vault.sol:148-154, contracts/core/Vault.sol:100-113, contracts/core/Vault.sol:133-143, contracts/core/Vault.sol:171-185 - Expected Behavior: Custody and liabilities remain solvent across transitions. - Observed Behavior: Managed assets account for on-contract + emergency custody; deposit/withdraw enforce exact transfer deltas; emergency migration preserves managed sum. - Status: COMPLIANT - Deviation Type: Invariant - Severity: INFO - Impact: Solvency model preserved under specified paths. - Remediation Direction: None.

[R9] - Spec Clause: I3 No Stored Surplus as independent liability state. - Code Reference: contracts/core/Vault.sol:23-25, contracts/core/Vault.sol:148-150 - Expected Behavior: Surplus not represented as separate liability ledger. - Observed Behavior: Only liabilities are balances and totalAssets; no surplus liability state variable exists. - Status: COMPLIANT - Deviation Type: Invariant - Severity: INFO - Impact: Liability model remains minimal/canonical. - Remediation Direction: None.

[R10] - Spec Clause: I4 ΔtotalAssets > 0 => ΔmanagedAssets == ΔtotalAssets. - Code Reference: contracts/core/Vault.sol:100-113 - Expected Behavior: Positive liability increments match custody increments exactly. - Observed Behavior: Deposit checks received == amount before applying state updates. - Status: COMPLIANT - Deviation Type: Invariant - Severity: INFO - Impact: Liability increase cannot outpace custody increase. - Remediation Direction: None.

[R11] - Spec Clause: I5 Emergency Neutrality: no mutation of totalAssets or user balances. - Code Reference: contracts/core/Vault.sol:160-190 - Expected Behavior: Emergency transition does not alter liabilities. - Observed Behavior: Emergency path changes only emergencyMode and emergencyCustodiedAssets; liabilities untouched. - Status: COMPLIANT - Deviation Type: Invariant - Severity: INFO - Impact: Accounting continuity preserved during emergency. - Remediation Direction: None.

[R12] - Spec Clause: I6 Initialization Safety: valid exactly once. - Code Reference: contracts/core/Vault.sol:31, contracts/core/Vault.sol:59-62, contracts/core/Vault.sol:73, contracts/core/Vault.sol:81 - Expected Behavior: Implementation locked; instance initialization single-use. - Observed Behavior: Constructor locks implementation; initialize guarded by _initialized. - Status: COMPLIANT - Deviation Type: Security - Severity: INFO - Impact: Prevents reinitialization misuse. - Remediation Direction: None.

[R13] - Spec Clause: Emergency trigger authority is governance-controlled through factory. - Code Reference: contracts/core/VaultFactory.sol:18, contracts/core/VaultFactory.sol:28-31, contracts/core/VaultFactory.sol:115 - Expected Behavior: Governance gate on emergency trigger function. - Observed Behavior: triggerEmergency restricted by onlyGovernance. - Status: COMPLIANT - Deviation Type: Security - Severity: INFO - Impact: Control plane aligns with doctrine. - Remediation Direction: None.

[R14] - Spec Clause: Factory calls vault.emergencyWithdraw() for registered vaults only. - Code Reference: contracts/core/VaultFactory.sol:116-117 - Expected Behavior: Registry check before emergency callout. - Observed Behavior: Reverts if !isVault[vault]; otherwise invokes vault emergency. - Status: COMPLIANT - Deviation Type: Security - Severity: INFO - Impact: Prevents arbitrary external emergency calls. - Remediation Direction: None.

[R15] - Spec Clause: Vault emergency transition sets mode, migrates balance, increments emergencyCustodiedAssets, leaves liabilities unchanged. - Code Reference: contracts/core/Vault.sol:168-185 - Expected Behavior: Full emergency custody migration semantics. - Observed Behavior: Mode set true; entire balance transferred; migrated amount added to emergencyCustodiedAssets; no liability mutation. - Status: COMPLIANT - Deviation Type: Functional - Severity: INFO - Impact: Hybrid custody accounting implemented. - Remediation Direction: None.

[R16] - Spec Clause: GOVERNANCE is immutable in VaultFactory. - Code Reference: contracts/core/VaultFactory.sol:18, contracts/core/VaultFactory.sol:37 - Expected Behavior: Immutable governance authority. - Observed Behavior: GOVERNANCE declared immutable and set only in constructor. - Status: COMPLIANT - Deviation Type: Security - Severity: INFO - Impact: Governance identity cannot be mutated post-deploy. - Remediation Direction: None.

[R17] - Spec Clause: Only governance may trigger emergency. - Code Reference: contracts/core/VaultFactory.sol:28-31, contracts/core/VaultFactory.sol:115 - Expected Behavior: Unauthorized callers blocked. - Observed Behavior: onlyGovernance enforced on triggerEmergency. - Status: COMPLIANT - Deviation Type: Security - Severity: INFO - Impact: Access control preserved. - Remediation Direction: None.

[R18] - Spec Clause: Only factory may execute vault emergency function. - Code Reference: contracts/core/Vault.sol:37-49, contracts/core/Vault.sol:160-164, contracts/core/Vault.sol:77 - Expected Behavior: Vault emergency callable only by bound factory. - Observed Behavior: onlyFactory modifier compares msg.sender to stored factory. - Status: COMPLIANT - Deviation Type: Security - Severity: INFO - Impact: Enforces factory trust boundary. - Remediation Direction: None.

[R19] - Spec Clause: Vault initialization emits VaultInitialized. - Code Reference: contracts/core/Vault.sol:83, contracts/libraries/VaultEvents.sol:5 - Expected Behavior: Initialization event emitted on successful initialization. - Observed Behavior: Emits VaultEvents.VaultInitialized. - Status: COMPLIANT - Deviation Type: Functional - Severity: INFO - Impact: Initialization observability present. - Remediation Direction: None.

[R20] - Spec Clause: Deposit emits Deposit. - Code Reference: contracts/core/Vault.sol:114, contracts/libraries/VaultEvents.sol:6 - Expected Behavior: Deposit transition must emit event. - Observed Behavior: Emits VaultEvents.Deposit(msg.sender, received). - Status: COMPLIANT - Deviation Type: Functional - Severity: INFO - Impact: Deposit traceability preserved. - Remediation Direction: None.

[R21] - Spec Clause: Withdraw emits Withdraw. - Code Reference: contracts/core/Vault.sol:145, contracts/libraries/VaultEvents.sol:7 - Expected Behavior: Withdraw transition must emit event. - Observed Behavior: Emits VaultEvents.Withdraw(msg.sender, amount). - Status: COMPLIANT - Deviation Type: Functional - Severity: INFO - Impact: Withdraw traceability preserved. - Remediation Direction: None.

[R22] - Spec Clause: Emergency custody migration emits EmergencyCustodyMigrated. - Code Reference: contracts/core/Vault.sol:11, contracts/core/Vault.sol:173-187 - Expected Behavior: Emergency custody migration transition emits migration event. - Observed Behavior: Event emitted only when balanceBefore > 0; no emission when emergency is activated with zero on-chain balance. - Status: PARTIAL - Deviation Type: Ambiguity - Severity: LOW - Impact: Monitoring systems may miss a zero-amount migration transition if they rely strictly on this event. - Remediation Direction: Clarify spec whether zero-amount emergency migration requires emission; if yes, emit EmergencyCustodyMigrated(0) unconditionally on emergency activation.

[R23] - Spec Clause: Emergency activation emits EmergencyActivated. - Code Reference: contracts/core/Vault.sol:189, contracts/libraries/VaultEvents.sol:8 - Expected Behavior: Emergency activation emits event. - Observed Behavior: Emits VaultEvents.EmergencyActivated(msg.sender) on each successful trigger. - Status: COMPLIANT - Deviation Type: Functional - Severity: INFO - Impact: Emergency activation observability present. - Remediation Direction: None.

[R24] - Spec Clause: Vault creation emits VaultCreated. - Code Reference: contracts/core/VaultFactory.sol:88, contracts/libraries/VaultEvents.sol:9 - Expected Behavior: Creation event with vault/salt linkage. - Observed Behavior: Emits VaultEvents.VaultCreated(vault, finalSalt). - Status: COMPLIANT - Deviation Type: Functional - Severity: INFO - Impact: Deterministic registry observability present. - Remediation Direction: None.

Invariant Alignment: - Liability Conservation: PASS - Solvency: PASS - No-liability-without-custody-delta: PASS - Emergency Neutrality: PASS - Initialization Safety: PASS

Trust-Boundary Alignment: - Factory Canonicality Model: ALIGNED - Governance Custody Assumptions: ALIGNED - Off-contract Recovery Separation: ALIGNED

Determinism Alignment: - CREATE2 Address Model: ALIGNED - Salt Derivation Model: ALIGNED - Registry Binding Model: ALIGNED

Spec Drift Analysis: - Undocumented behaviors present: YES - Spec requirements unimplemented: NO - Ambiguity materially affecting review: YES

Final Verdict: REQUIRES SPEC OR CODE REVISION

End of Report. FORMAL MODEL CONFORMANCE REPORT

Model Version: v1.0 (docs/formal_model_v1.md)

Code Baseline: 696468907a9ff0dd0e37cee85c0829581bfdc9be (working tree with local modifications)

Overall Mathematical Conformance: CONFORMANT

Equation Coverage Summary: - Total equations: 9 - Satisfied: 9 - Violated: 0 - Partial: 0 - Not applicable: 0

Critical Equation Failures: - None.

High-Risk Equation Gaps: - None.

Equation Matrix:

[E1] - Formal Equation: $MA(t) = OC(t) + EC(t)$ - Variable Mapping:
MA -> managedAssets(),
OC -> IERC20(underlying).balanceOf(address(this)),
EC -> emergencyCustodiedAssets - Transition Context: Global (all states) - State Definition: S(t)={TA,EC,B[u],OC,MA,EM,INIT} - Expected Delta Relationship: Identity definition holds at every read of MA - Observed Code Behavior: managedAssets() returns balanceOf(this) + emergencyCustodiedAssets in Vault.sol - Status: SATISFIED - Violation Type: None - Severity: INFO - Impact: None - Remediation Direction: None

[E2] - Formal Equation: $TA(t) = \Sigma_u B[u](t)$ - Variable Mapping:
TA -> totalAssets, B[u] -> balances[u] - Transition Context: deposit,

withdraw, emergencyWithdraw, initialize - State Definition: S(t) -> S(t+1) over protocol transitions - Expected Delta Relationship: ΔTA = ΔB[user] on deposit/withdraw; no TA/B mutation on emergency/init (except initial zero state) - Observed Code Behavior: deposit adds same received to balances[msg.sender] and totalAssets; withdraw subtracts same amount; emergencyWithdraw and initialize do not mutate TA/B - Status: SATISFIED - Violation Type: None - Severity: INFO - Impact: None - Remediation Direction: None

[E3] - Formal Equation: MA(t) >= TA(t) - Variable Mapping: MA -> managedAssets(), TA -> totalAssets - Transition Context: Global solvency invariant - State Definition: S(t) -> S(t+1) for all valid transitions - Expected Delta Relationship: Deposits and withdrawals move assets and liabilities in lockstep; emergency migration preserves MA - Observed Code Behavior: Exact transfer checks in deposit/withdraw; emergencyWithdraw migrates full on-chain balance into EC; solvency() computes managedAssets() >= totalAssets - Status: SATISFIED - Violation Type: None - Severity: INFO - Impact: None - Remediation Direction: None

[E4] - Formal Equation: Deposit x: TA+ = x, B[user]+ = x, OC+ = x, EC unchanged - Variable Mapping: x -> amount (validated as received==amount), TA -> totalAssets, B[user] -> balances[msg.sender], OC -> token balance, EC -> emergencyCustodiedAssets - Transition Context: deposit(uint256) - State Definition: S(t+1)={TA+x,EC,B[user]+x,OC+x,MA+x,EM,INIT} - Expected Delta Relationship: ΔTA=ΔB[user]=ΔOC=x, ΔEC=0 - Observed Code Behavior: transferFrom; compute received; require received==amount; then balances += received, totalAssets += received; no EC mutation - Status: SATISFIED - Violation Type: None - Severity: INFO - Impact: None - Remediation Direction: None

[E5] - Formal Equation: Withdraw x: TA- = x, B[user]- = x, OC- = x, EC unchanged - Variable Mapping: x -> amount, TA -> totalAssets, B[user] -> balances[msg.sender], OC -> token balance, EC -> emergencyCustodiedAssets - Transition Context: withdraw(uint256) - State Definition: S(t+1)={TA-x,EC,B[user]-x,OC-x,MA-x,EM,INIT} - Expected Delta Relationship: ΔTA=ΔB[user]=ΔOC=-x, ΔEC=0 - Observed Code Behavior: Balance sufficiency check; decrement balances and totalAssets; transfer out; require sent==amount; no EC mutation - Status: SATISFIED - Violation Type: None - Severity: INFO - Impact: None - Remediation Direction: None

[E6] - Formal Equation: Emergency with m=OC(t): EM=true, EC+=m, OC=0, TA unchanged, B[u] unchanged - Variable Mapping: EM -> emergencyMode, EC -> emergencyCustodiedAssets, OC -> token balance, TA -> totalAssets, B[u] -> balances[u] - Transition Context: emergencyWithdraw() - State Definition: S(t+1)={TA,EC+m,B[u],0,EC+m,true,INIT} - Expected Delta Relationship: ΔEM=true, ΔEC=+m, ΔOC=-m, ΔTA=0, ΔB[u]=0 - Observed Code Behavior: Sets emergencyMode=true; reads balanceBefore; transfers full balanceBefore to custodian; requires migrated==balanceBefore; increments emergencyCustodiedAssets by migrated; no TA/B mutation - Status: SATISFIED - Violation Type: None - Severity: INFO - Impact: None - Remediation Direction: None

[E7] - Formal Equation: INIT one-way false -> true once per clone; never true -> false - Variable Mapping: INIT -> _initialized - Transition Context: initialize(), constructor lock on implementation - State Definition: Clone state INIT=false pre-init, INIT=true post-init - Expected Delta Relationship: Single successful init transition only - Observed Code Behavior: initialize reverts if _initialized; sets _initialized=true; no function sets false; constructor sets _initialized=true on implementation contract - Status: SATISFIED -

Violation Type: None - Severity: INFO - Impact: None - Remediation Direction: None

[E8] - Formal Equation: SALT = keccak256(abi.encode(SALT_DOMAIN, chainid, factory, underlying, admin, userSalt)) - Variable Mapping: SALT_DOMAIN -> DeterministicSalt.SALT_DOMAIN, factory -> address(this) in factory call, admin -> custodian parameter, userSalt -> userSalt - Transition Context: createVault, predictVaultAddress - State Definition: Deterministic identity derivation in S(t) independent of TA/B transitions - Expected Delta Relationship: Same input tuple yields same finalSalt - Observed Code Behavior: deriveSalt encodes exact tuple (SALT_DOMAIN, block.chainid, factory, underlying, admin, userSalt) and hashes with keccak256 - Status: SATISFIED - Violation Type: None - Severity: INFO - Impact: None - Remediation Direction: None

[E9] - Formal Equation: predictVaultAddress(inputs) = createVault(inputs) address outcome (same context) - Variable Mapping: inputs -> (underlying, custodian, userSalt), context includes same factory + implementation - Transition Context: predictVaultAddress and createVault - State Definition: S(t) pre-create with unused salt path - Expected Delta Relationship: Predicted deterministic clone address equals deployed clone address - Observed Code Behavior: Both paths derive same finalSalt; both use Clones.predictDeterministicAddress(..., address(this)); createVault deploys cloneDeterministic with same implementation/salt/deployer - Status: SATISFIED - Violation Type: None - Severity: INFO - Impact: None - Remediation Direction: None

Invariant Verification: - I1 Liability Conservation: PASS - I2 Solvency: PASS - I3 No Stored Surplus: PASS - I4 No-liability-without-custody-delta: PASS - I5 Emergency Neutrality: PASS - I6 Initialization Safety: PASS

State Space Soundness: - Non-negativity preserved: YES - Overflow safety preserved: YES - Monotonicity constraints respected: YES - Non-interference validated: YES - Composition closure verified: YES

Transition Proof Status: - deposit(): VERIFIED - withdraw(): VERIFIED - emergencyWithdraw(): VERIFIED - initialize(): VERIFIED

Final Verdict: MATHEMATICALLY SOUND

End of Report. ECONOMIC RISK CLASSIFICATION REPORT

Baseline Context: - TVL assumption: UNQUANTIFIED – DATA GAP; normalized model used (TVL = 1.00x) for comparability. - Asset liquidity assumption: Two regimes modeled: high-liquidity (low unwind slippage) and low-liquidity (higher recovery haircut and delay). - Custody model assumption: Partial external custody after emergency (emergencyCustodian off-contract). - Governance response latency: Assumed 4–24 hours multisig coordination (UNQUANTIFIED – DATA GAP). - Cross-protocol exposure: No direct integrations evidenced in provided reports; contagion treated as indirect/reputational.

Overall Economic Risk Posture: UNACCEPTABLE

Top Economic Risks (Ranked by EL): 1. Emergency-mode fund lock / no on-chain redemption path (MR-MJ-01) 2. Solvency overstatement from unverifiable off-contract custody accounting (MR-MJ-02) 3. User capital routing to unsafe custodian configurations via permissionless vault creation (MR-MJ-03)

Risk Matrix:

[ER-01] - Source Finding ID: MR-MJ-01 (contracts/core/Vault.sol:160) - Technical Root Cause: Emergency activation disables normal flows and migrates assets to external custodian without on-chain user redemption mechanism. - Exploit / Failure Scenario: Emergency trigger causes protocol-wide inability for users to redeem on-chain; recovery depends on external custodian/governance process. - Capital at Risk (min/base/stress): 0.30x / 0.70x / 1.00x TVL - Likelihood: 3 - Impact: 5 - Exposure Multiplier: 1.5 - Risk Score: 22.5 - Expected Loss (EL): 0.42x TVL - Economic Severity: SYSTEMIC - Time to Materialization: RAPID (immediate on emergency trigger) - Reversibility: Partial - Systemic Amplification: YES - Mitigation Priority: P0 - Responsible Owner: Protocol

[ER-02] - Source Finding ID: MR-MJ-02 (contracts/core/Vault.sol:148) - Technical Root Cause: managedAssets() counts emergencyCustodiedAssets as available despite off-contract unverifiability. - Exploit / Failure Scenario: Reported solvency remains overstated while real recoverable assets are impaired/delayed, causing delayed loss recognition and potential bank-run dynamics. - Capital at Risk (min/base/stress): 0.10x / 0.40x / 1.00x TVL - Likelihood: 3 - Impact: 4 - Exposure Multiplier: 1.5 - Risk Score: 18.0 - Expected Loss (EL): 0.24x TVL - Economic Severity: CRITICAL - Time to Materialization: GRADUAL to RAPID (depends on redemption pressure) - Reversibility: Partial - Systemic Amplification: YES - Mitigation Priority: P0 - Responsible Owner: Protocol

[ER-03] - Source Finding ID: MR-MJ-03 (contracts/core/VaultFactory.sol:45) - Technical Root Cause: Permissionless vault instantiation with arbitrary custodian addresses; safety depends on off-chain allowlisting/discovery. - Exploit / Failure Scenario: Users route funds into vaults with malicious/unsafe custodian parameters through spoofed discovery surfaces. - Capital at Risk (min/base/stress): 0.01x / 0.08x / 0.25x TVL - Likelihood: 4 - Impact: 3 - Exposure Multiplier: 1.25 - Risk Score: 15.0 - Expected Loss (EL): 0.064x TVL - Economic Severity: HIGH - Time to Materialization: GRADUAL - Reversibility: Partial - Systemic Amplification: NO - Mitigation Priority: P1 - Responsible Owner: Ops

[ER-04] - Source Finding ID: SPEC-R22 (contracts/core/Vault.sol:173-187) - Technical Root Cause: Zero-balance emergency transition may not emit EmergencyCustodyMigrated, reducing monitoring completeness. - Exploit / Failure Scenario: Monitoring misses emergency state transition edge case; delayed operational response increases secondary loss risk. - Capital at Risk (min/base/stress): 0.00x / 0.02x / 0.05x TVL - Likelihood: 2 - Impact: 2 - Exposure Multiplier: 1.0 - Risk Score: 4.0 - Expected Loss (EL): 0.008x TVL - Economic Severity: LOW - Time to Materialization: GRADUAL - Reversibility: Full - Systemic Amplification: NO - Mitigation Priority: P2 - Responsible Owner: Ops

Portfolio-Level View: - Aggregate downside (base case): 0.78x TVL (pre-overlap); practical capped downside <= 1.00x TVL - Aggregate downside (stress case): 1.00x TVL - Aggregate Expected Loss: ~0.55x TVL (overlap-adjusted) - Insolvency risk: HIGH - Liquidity run risk: HIGH - Contagion risk: MEDIUM

Kill-Switch Threshold Analysis: - TVL loss threshold triggering halt: >=10% realized impairment or any confirmed custodian non-performance. - Liquidity depletion threshold: on-chain liquidity coverage OC/TA < 1.00 sustained for one governance epoch. - Governance intervention threshold: any emergency activation without pre-defined, enforceable redemption runbook and ETA.

Decision Guidance: - Deploy now: NO - Conditions required before deploy: On-chain or cryptographically enforceable post-emergency redemption path; solvency metric split between on-chain and externally custodied recoverable assets; trusted vault discovery/allowlist controls. - Immediate mitigations (P0): Add emergency redemption mechanism; prevent solvency overstatement (separate recoverableExternalAssets with conservative haircuts); define enforceable custody SLAs and proofs-of-reserve/process attestations. - Near-term mitigations (P1): Restrict factory creation or gate official registry listing; add user-facing vault authenticity checks; formalize emergency recovery timeline guarantees. - Monitoring requirements post-deploy: Real-time OC/TA and external custody coverage dashboards; emergency-state alerts independent of zero-amount migration event; governance latency and custodian response SLO tracking.

Final Verdict: DO NOT DEPLOY — ECONOMIC RISK UNACCEPTABLE

End of Report. DEPLOYMENT READINESS DECISION REPORT

Code Baseline: - Commit / Tag: 696468907a9ff0dd0e37cee85c0829581bfdc9be / v1.0.0-preaudit - Spec Version: v1.0 (docs/spec_v1.md, reports/spec.md) - Model Version: v1.0 (docs/formal_model_v1.md, reports/formal.md)

Release Context: - Target Network: Ethereum mainnet (docs/deployment_context_v1.md) - Deployment Window: Not specified - Responsible Owners: Governance multisig 0x1111111111111111111111111111111111111111 (placeholder; no named individuals) - Monitoring Stack: On-chain event indexer (VaultCreated, Deposit, Withdraw, EmergencyCustodyMigrated, EmergencyActivated), invariant monitor worker, alert router (PagerDuty/Slack placeholder), severity classes P0/P1/P2 - Rollback Mechanism: Freeze integrations/front-end, trigger vault emergency via governance, reconcile custody ledger, publish incident report, re-run full agent review (docs/deployment_context_v1.md)

Gate Evaluation: - Structural Gate: PASS - Formal Compliance Gate: PASS - Mathematical Gate: FAIL - Economic Gate: FAIL - Operational Gate: FAIL

Readiness Score: - Structural: 70 - Formal: 72 - Economic: 15 - Operational: 45 - Total: 53.1

Decision Matrix:

[Structural] - Source Report: reports/master.md, reports/full-report.md - Status: PARTIAL - Blocking: NO - Evidence Reference: reports/master.md (Overall Structural Integrity: REQUIRES REVISION; no critical findings) - Residual Risk: Major architectural risks remain (emergency redemption path, solvency overstatement, permissionless custodian exposure). - Required Action: Resolve MR-MJ-01/02/03 and re-issue MASTER verdict as SAFE. - Owner: Protocol - Due Date: 2026-03-06

[Formal Compliance] - Source Report: reports/spec.md - Status: PARTIAL - Blocking: NO - Evidence Reference: reports/spec.md (PARTIALLY COMPLIANT;

R22 PARTIAL; Final Verdict: REQUIRES SPEC OR CODE REVISION) - Residual Risk: Spec ambiguity on emergency event semantics can cause integration drift. - Required Action: Publish spec clarification/version bump for emergency-event semantics and error/event surface. - Owner: Protocol + Governance - Due Date: 2026-03-06

[Mathematical] - Source Report: reports/formal.md, reports/full-report.md (formal section) - Status: FAIL - Blocking: YES - Evidence Reference: reports/full-report.md (Formal section: NON-CONFORMANT, E5/E6 violated; transition proofs failed for withdraw/emergency) - Residual Risk: Unresolved contradiction across formal evidence; invariant assurance is not governance-grade final. - Required Action: Re-run FORMAL_MODEL_AGENT on immutable clean baseline; clear E5/E6 dispute with reproducible proofs. - Owner: Formal Methods + Protocol - Due Date: 2026-03-04

[Economic] - Source Report: reports/risk.md - Status: FAIL - Blocking: YES - Evidence Reference: reports/risk.md (Overall Economic Risk Posture: UNACCEPTABLE; Final Verdict: DO NOT DEPLOY) - Residual Risk: Aggregate expected loss ~0.55x TVL; systemic emergency-mode and custody-accounting risks. - Required Action: Implement P0 mitigations (enforceable emergency redemption path, solvency metric hardening, custodian safety controls) and reclassify posture. - Owner: Protocol + Risk + Governance - Due Date: 2026-03-06

[Operational] - Source Report: docs/deployment_context_v1.md, reports/full-report.md - Status: FAIL - Blocking: YES - Evidence Reference: docs/deployment_context_v1.md (monitoring/rollback/IR defined, but rollback test evidence absent; owner identities placeholder) - Residual Risk: Accountability and execution readiness not fully verifiable before mainnet deployment. - Required Action: Assign named owners, test rollback runbook, archive drill evidence, finalize incident command contacts. - Owner: Governance + Ops - Due Date: 2026-03-03

Open Blockers (P0): - Economic posture is UNACCEPTABLE (reports/risk.md). - Mathematical evidence is not cleanly resolved across prior reports (reports/full-report.md formal section vs reports/formal.md). - No tested rollback evidence and no named accountable owner roster for incident execution. - Emergency-mode fund availability and solvency-accounting architecture risks remain open (reports/master.md, reports/risk.md).

Required Preconditions Before Deploy: - Clear all P0 economic risks and obtain updated ACCEPTABLE economic posture. - Produce single-source formal conformance report on immutable clean baseline with all critical transitions PASS. - Complete and evidence a tested rollback exercise. - Publish named owner/accountability matrix and incident escalation contacts. - Record governance-approved residual expected loss threshold and acceptance policy.

Risk Acceptance Register: - Accepted Risk: None recorded - Economic Exposure: N/A - Approver: N/A - Expiration Date: N/A - Monitoring Requirement: N/A

Post-Deploy Monitoring Requirements: - Invariant Monitoring: Continuous checks for totalAssets == sum(balances), managedAssets() >= totalAssets, registry consistency. - TVL Monitoring: Real-time impairment and custody-coverage drift alerts. - Liquidity Monitoring: Alert on OC/TA < 1.00 sustained for one governance epoch. - Alert Thresholds: P0 on any invariant breach, failed emergency reconciliation, or confirmed custodian non-performance.

Kill-Switch Conditions: - Trigger Conditions: Any confirmed invariant break, custody/accounting divergence, emergency reconciliation failure, or severe liquidity impairment. - Authorized Executor: Governance multisig only. - Execution Path: VaultFactory.triggerEmergency(vault) plus incident runbook actions in docs/deployment_context_v1.md.

Final Decision: NO_GO

Decision Rationale: Mandatory gate failures exist. Economic Gate fails (UNACCEPTABLE posture in reports/risk.md), Mathematical Gate fails due unresolved critical formal evidence conflict across prior reports, and Operational Gate fails due missing tested rollback and incomplete owner accountability. Under hard rules, any mandatory gate FAIL results in automatic NO_GO.

Re-evaluation Trigger: - Condition: Updated MASTER/SPEC/FORMAL/RISK package on immutable baseline shows all mandatory gates PASS and governance signs residual risk acceptance threshold. - Target Date: 2026-03-06

End of Report.