Commit-bound scope.
Ready for an audit quote.

Synthetic founding-pilot sample tied to one frozen repository identifier. This document prepares scope and supporting evidence; it is not a smart contract audit, vulnerability assessment, or security assurance.

ARTIFACT	STATE	CHAIN	REVIEW TARGET
audit_scope_readiness.v1	QUOTE_READY	Base	Independent smart contract audit

Repository anchor

`https://github.com/Vetassikc/Vartovii`

`Pinned commit: 55effcaaa01a7569d7cd483ca18b5e6b50392b9b`

`Build: forge build · Test: forge test`

Scope manifest

IN SCOPE	OUT OF SCOPE
src/TreasuryVault.sol src/RoleRegistry.sol	script/ deployment operations

Evidence register

Every factual entry carries a source or artifact reference and a checked timestamp. Statuses describe documentation support, not code safety.

CATEGORY	STATUS	SOURCE / CHECKED	NOTE
Repository Identity	EVIDENCED	https://github.com/Vetassikc/Vartovii/tree/55effcaaa01a7569d7cd483ca18b5e6b50392b9b/examples/vartovii-audit-scope-demo 2026-07-10T12:00:00Z	Repository identity, chain, commit, and in-scope source paths are explicit.
Privileged Roles And Upgrades	PARTIAL	src/RoleRegistry.sol 2026-07-10T12:04:00Z	Roles are visible, but deployed admin addresses and upgrade ownership evidence are absent.
Incident And Disclosure Readiness	MISSING	No direct artifact found 2026-07-10T12:08:00Z	No SECURITY.md or private disclosure path was found in the synthetic fixture.

Architecture and actor map

TreasuryVault holds native assets. RoleRegistry identifies operator and emergency-operator roles. The delivery asks the protocol team to reconcile these source roles with deployed addresses and any upgrade authority.

Auditor-ready RFQ summary

Quote a review of TreasuryVault.sol and RoleRegistry.sol at the pinned commit on Base. Confirm assumptions for privileged roles, deployment reconciliation, dependency review, and remediation follow-up.

Prioritized gaps

These are missing handoff artifacts and their audit-scoping impact. They are not vulnerability findings.

PRIORITY	OWNER	REQUIRED ARTIFACT	AUDIT-SCOPING IMPACT
P1	Protocol team	Deployed proxy and admin addresses	The auditor cannot reconcile privileged actors with the proposed scope.
P1	Protocol team	Upgrade and emergency-action owner map	Quote questions remain open around upgradeable components and response authority.
P2	Protocol team	SECURITY.md and disclosure contact	The handoff lacks an incident and disclosure path.
P2	Lead engineer	Dependency exception notes	The auditor must rediscover why selected packages are pinned.
P2	Lead engineer	Deployment manifest by chain	The review target cannot be matched cleanly to deployed instances.

Delivery boundary

No guarantee of audit acceptance, audit price, grant approval, vulnerability discovery, launch safety, or security outcome. Prepared by: Vartovii scope analyst.

This synthetic artifact prepares audit scope and supporting evidence. It is not a smart contract audit, vulnerability assessment, or security assurance.