anchor@anchor-cyber:~$ audit --framework=any --trust=verify

ANCHOR CYBER SECURITY LLC

Audit Fieldwork — Trust but Verify

The framework-agnostic version of Anchor's audit methodology — same discipline whether the framework is CSF, SOC 2, or ISO 27001.

$ audit --phases

The Eight Phases

0 Independent access

Your own read access to the real systems — client consoles, source repos, live queries. Never evidence mediated entirely through the client's own export or script output.

1 Rebuild context from zero

Independently trace assets, data flows, and scope — don't start from the client's own system-description document as ground truth.

2 Verify every control claim

For each "Implemented" claim: documentary evidence AND a live/runtime test AND, where possible, an interview — triangulate, don't accept one source.

3 Independent risk scoring

Score likelihood/impact from what you found in Phase 2, before reading the client's own risk register. Reconcile after, not before.

4 External artifact collection

Signed contracts, insurance policies, console configurations — things no repository or export can produce. Get the originals.

5 Resolve legal exposure empirically

Don't ask whether regulated data touched an unauthorized system — query it and check.

6 Delta report, not adoption

Your own findings first; diff against any client self-assessment second. The self-assessment is a cross-check on your work, not the source of it.

7 Re-verify remediation

"Done" gets tested in production, by you, before it's closed in the final report — not accepted on the client's word.

$ audit --evidence-tiers

Evidence Hierarchy

TIER	EXAMPLE	WEIGHT
Weakest	Client's own written claim, unverified	Starting hypothesis only
Weak	Screenshot or document the client selected and provided	Corroborating, not sufficient alone
Strong	Live query or test you ran yourself against the real system	Primary evidence
Strongest	Independently reproducible result, or a signed third-party document (contract, cert)	Closes the finding

THE ONE RULE UNDERNEATH ALL EIGHT PHASES

Anywhere a client's documentation says "verify with this command" or "see this file," treat that as a suggested starting point for your own independent test — never as the test itself. A self-assessment that tells you exactly where to look is still worth checking what it didn't point you to.

src: Anchor's internal audit methodology, generalized from framework-specific practice exit 0