

CyberAssess

Annual Security Review and Risk Assessment

CyberAssess is the annual cycle that keeps a security program current. It re-runs the same assessment that established your baseline — all 106 NIST CSF 2.0 subcategories, six-level CMMI-aligned maturity scoring, FAIR exposure modeling — and measures what actually moved since last year.

SecureStart establishes the baseline. CyberAssess keeps it honest: remediation verified rather than assumed, the risk register refreshed, the roadmap rebuilt for the next twelve months, and current evidence on hand when an insurer, a customer or the board asks.

WHY CLIENTS BUY THIS NOW

THE ANNUAL CYCLE

Insurance renewal, an audit, a customer review or a board calendar requires a current, independent assessment every year.

LAST YEAR'S ROADMAP

Remediation was funded and worked. Nobody has independently verified what closed and what quietly did not.

THE ENVIRONMENT MOVED

New systems, new vendors, new AI tooling, an acquisition or growth has changed the risk picture the baseline was built on.

WHAT THE ANNUAL REVIEW COVERS

The full assessment re-run against a changed environment, plus the three things a baseline assessment cannot give you: verified progress, trend, and a refreshed plan.

► Full NIST CSF 2.0 re-assessment

All 106 subcategories re-rated across Govern, Identify, Protect, Detect, Respond and Recover — same method, same scale, comparable results.

► Remediation validation

Independent verification of what last year's roadmap actually closed, what partially closed, and what reopened.

► Quantified exposure update

FAIR annualized loss exposure recalculated, so the dollar figure in front of the board reflects the current environment.

► Evidence pack

Current assessment, scorecard and roadmap packaged for insurers, enterprise customers and auditors who ask for a recent independent review.

► Maturity trend and delta

Year-over-year movement by Function and subcategory, so progress is measurable rather than asserted.

► Risk register refresh

Organizational, technical and operational risks re-identified and re-scored, with new entries for what changed during the year.

► Third-party and AI exposure

Changes in the critical vendor set and in AI tooling adopted during the year, assessed as part of the cycle.

► Executive and board readout

A live session on what moved, what did not, and what to fund next.

WHAT YOU RECEIVE EACH CYCLE

- **Updated maturity scorecard** — all 106 subcategories rated, with the prior year shown alongside.
- **Remediation validation report** — what closed, what did not, and what reopened.
- **Refreshed risk register** — re-scored, with remediation recommendations and named owners.
- **Updated exposure model** — FAIR annualized loss exposure recalculated against the current environment.
- **Twelve-month roadmap** — costed and sequenced, carrying forward what remains open.
- **Executive and board briefing** — delivered live, plus a reusable briefing pack.

Annual

recurring review cycle

106

NIST CSF 2.0 subcategories re-rated

Year over year

measurable maturity delta

STANDARDS AND METHODS APPLIED

STANDARD / AUTHORITY	APPLIED TO
NIST CSF 2.0	Assessment spine — all 106 subcategories across the six Functions
CMMI-aligned maturity model	Six-level scoring, held constant year over year for comparability
FAIR (Factor Analysis of Information Risk)	Annualized loss exposure and scenario modeling
ISO 31000:2018	Risk criteria, scoring and treatment
NIST SP 800-53 Rev. 5; ISO/IEC 27001:2022	Control reference and certification crosswalk
NIST AI RMF 1.0	AI tooling adopted during the review period

DELIVERY APPROACH

1 DISCOVERY Re-scope against what changed: systems, vendors, people, acquisitions, AI adoption. Days 1-3	2 ASSESSMENT Structured interviews and evidence review across all six Functions. Days 4-10	3 VALIDATION Independent verification of prior-year remediation; maturity delta and FAIR update. Days 11-15	4 REPORTING Report build, QA, named-assessor sign-off, executive and board readout. Days 16-21	5 INTERIM ADVISORY Elective quarterly check-ins, remediation oversight and roadmap tracking between cycles. Elective
--	--	---	--	--

TIMELINE Three to four weeks per cycle, run annually. Most clients anchor the cycle to an insurance renewal or board calendar. Elective quarterly check-ins keep the roadmap current in between.

WHERE AI IS USED – AND WHERE IT IS NOT

- Evidence and document review is AI-accelerated, and prior-year artifacts are compared automatically so the review focuses on what changed rather than re-reading everything.
- Control mapping and crosswalking to 800-53, ISO 27001 and client frameworks is model-assisted, then assessor-verified.
- Maturity delta and roadmap costing are generated from structured data, which keeps a recurring review economical year after year.
- **Every rating, every dollar figure and every validation decision is reviewed and signed by a named CDA assessor.** Client data is not used to train external models.

WHO BUYS IT

CEO and COO · CISO, CIO and CTO · Chief Risk Officer · General Counsel · Compliance Officer · Audit committee and board · PE operating partners

IDEAL CLIENT PROFILE

Organizations that have already established a security baseline and need to keep it current — typically 50 to 1,000 employees in regulated or contract-driven sectors, with annual insurance, audit or customer-review obligations and no internal capacity to run an independent assessment. Also available as the annual risk assessment attached to a CyberComply subscription.

WHY CDA

► Comparable, not just current

The same method and the same scale every year, so the board sees a trend line instead of four unrelated assessments.

► Progress verified independently

Remediation is confirmed closed by someone who did not do the remediation — which is what an insurer or auditor is actually asking for.

► A roadmap that carries forward

Each cycle updates the plan rather than starting a new one, so open items stay visible until they close.

► Cheaper every year

The baseline is already built. Recurring cycles cost less than first-year work while producing the same evidence.

SCOPE, GUARDRAILS AND RESPONSIBLE AI

Non-invasive and evidence-based; penetration testing and other intrusive work is scoped separately through CyberRecon. Evidence is held under NDA in CDA's environment. AI-assisted analysis is reviewed and signed by a named CDA assessor; client data is not used to train external models. Not a certification or audit opinion.

Scope it with us.

Engagements are scoped and fixed-fee quoted to your environment. Contact us for scoping, references and a sample deliverable.

833-54-CYBER (833-542-9237)

info@cyberdefenseadvisors.com
cyberdefenseadvisors.com