

# SecureStart™

## Independent Cyber Risk Assessment

SecureStart is a fixed-scope, independently delivered cyber risk assessment that tells an executive team three things in three weeks: where the program actually stands against NIST CSF 2.0, what the exposure is worth in dollars, and what to fix first.

It is scoped for companies that need a defensible answer fast — for an insurance renewal, a customer questionnaire, a board that has started asking — without committing to a multi-month engagement. Roughly six hours of client time, start to readout.

### WHY CLIENTS BUY THIS NOW

#### INSURANCE

A carrier or broker is asking for evidence of controls at renewal, and the application questions have outrun what the team can answer from memory.

#### CUSTOMERS & CONTRACTS

A security questionnaire, a vendor review or a prime contractor's flow-down requirement has landed, and there is no current assessment to point at.

#### BOARD & OWNERSHIP

A board, an investor or a new executive has asked what the cyber risk is — in business terms, not control counts.

### WHAT GETS ASSESSED

All 106 subcategories of NIST CSF 2.0, rated on a six-level CMMI-aligned maturity scale, across the six Framework Functions.

#### ► Govern

Strategy, roles, policy, oversight, and how cyber risk reaches the board.

#### ► Protect

Identity and access, awareness, data security, platform security, resilience of technology.

#### ► Respond

Incident response plan, roles, communications, analysis, mitigation, lessons learned.

#### ► Identify

Asset and data inventory, business environment, risk assessment practice, supplier risk.

#### ► Detect

Monitoring coverage, logging, alerting, and how anomalies are actually adjudicated.

#### ► Recover

Recovery planning, execution, and communications — tested against real scenarios.

### WHAT YOU RECEIVE

- **Maturity scorecard** — all 106 NIST CSF 2.0 subcategories rated, with current and target state.
- **Quantified exposure model** — annualized loss exposure using FAIR, so risk is stated in dollars.
- **Costed remediation roadmap** — phased, sequenced, with effort and investment attached to each item.
- **Executive readout** — a 60-minute session for the leadership team and, where asked, the board.
- **Board-ready summary** — a short narrative a non-technical director can read and act on.

**3 weeks**

kickoff to executive readout

**~6 hours**

of client time, start to finish

**106**

NIST CSF 2.0 subcategories rated

## 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, so progress is measurable year over year       |
| FAIR (Factor Analysis of Information Risk) | Annualized loss exposure and scenario modeling                    |
| NIST SP 800-53 Rev. 5                      | Control reference for remediation design                          |
| ISO/IEC 27001:2022                         | Crosswalk for clients heading toward certification                |
| ISO 31000:2018                             | Risk criteria, scoring and treatment discipline                   |

## DELIVERY APPROACH

|                                                                                                                             |                                                                                                                          |                                                                                                                          |                                                                                                                             |                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1</b><br><b>DISCOVERY</b><br>Kickoff, scoping confirmation, document request, stakeholder scheduling.<br><b>Days 1-3</b> | <b>2</b><br><b>ASSESSMENT</b><br>Structured interviews and evidence review across all six Functions.<br><b>Days 4-10</b> | <b>3</b><br><b>ANALYSIS</b><br>Maturity scoring, FAIR modeling, prioritization and roadmap costing.<br><b>Days 11-15</b> | <b>4</b><br><b>REPORTING</b><br>Report build, internal QA, named-assessor sign-off, executive readout.<br><b>Days 16-21</b> | <b>5</b><br><b>ONGOING ADVISORY</b><br>Optional remediation oversight, re-assessment, or fractional security leadership.<br><b>Elective</b> |
|-----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|

**TIMELINE** Three weeks from kickoff to executive readout. Approximately six hours of client time.

## WHERE AI IS USED – AND WHERE IT IS NOT

- Evidence and document review is AI-accelerated: policies, prior audits, configuration exports and questionnaire responses are parsed and mapped to CSF subcategories in a fraction of manual review time.
- Control mapping and crosswalking to 800-53, ISO 27001 and client frameworks is model-assisted, then assessor-verified.
- Narrative drafting and roadmap costing are accelerated so more of the engagement budget goes to analysis.
- **Every rating, every dollar figure and every recommendation is reviewed and signed by a named CDA assessor.** AI does not score, and it does not sign.

## 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

Companies from roughly 50 to 1,000 employees in regulated or contract-driven sectors — financial services, healthcare, insurance, legal, construction and AEC, manufacturing, professional services, and PE portfolio companies — that have IT leadership but no full-time security executive.

## WHY CDA

## ► Independent by construction

CDA sells no security products and resells no managed service that the assessment could conveniently recommend. The finding is the finding.

## ► Quantified, not color-coded

FAIR loss modeling turns a heat map into a number a CFO can weigh against the cost of fixing it.

## ► A named assessor, not a platform

A senior practitioner owns the engagement and signs the report. Scanning tools and SaaS dashboards do not produce a defensible opinion.

## ► Built to be handed on

The client owns the report and the roadmap and may take either to any provider, including a competitor.

## SCOPE, GUARDRAILS AND RESPONSIBLE AI

Non-invasive and evidence-based; intrusive testing requires separate written authorization. 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