FCI

FIRM SECURITY

SECURITY ASSESSMENTS

Start with a clear picture of where you stand.

FCI assesses your firm's current security posture — identifying gaps, vulnerabilities, and exposure across four dimensions. Whether you need exam-ready evidence, a baseline before onboarding, or a clear answer to "where do we stand?" — this is where it starts.

30+	400+	4
years serving financial services	firms assessed	assessment dimensions

WHY IT MATTERS

Every firm has a security posture. Most don't know what theirs actually looks like.

Financial regulators expect firms to maintain cybersecurity policies, conduct vulnerability assessments, and produce evidence of ongoing controls. Broker-dealers and insurance carriers ask the same questions. They want to know their branch offices or agencies are protected. The problem is that most firms don't have a clear picture of where they stand until someone asks — and by then, the timeline is already running.

FCI's security assessments give firms that picture before it becomes urgent. Whether your firm is preparing for an exam, renewing cyber insurance, responding to a home office request, or simply trying to understand its current exposure — FCI provides the assessment, the evidence, the remediation recommendations, and the context to make informed decisions.

> THE QUESTION EVERY FIRM SHOULD BE ABLE TO ANSWER
>
> *Can you show me your last vulnerability scan and network penetration test results?*

FOUR ASSESSMENT DIMENSIONS

A complete view of your firm's security posture.

FCI assesses firms across four dimensions. Each dimension targets a different part of the firm's environment and produces its own set of findings and evidence. Firms can engage FCI for one dimension or all four — depending on what they need and what their regulator, insurer, or home office requires.

DIMENSION 1

Gap Analysis

A 30-minute assessment of what controls are in place, what is missing, and what your next exam or renewal will require. No cost, no commitment — just a clear picture of where you stand today.

30 Minutes · Free · No Commitment

DIMENSION 2

Network Pen Testing & Vulnerability Scan

Penetration testing and vulnerability scanning across your internal and external network as well as for your endpoints — evidence your examiner will accept.

External Network · Internal with Endpoints · Exam-Ready Evidence

DIMENSION 3

Public-Facing Assessment

External scan of your firm's internet-facing attack surface — DNS, web properties, email configuration, and exposed services. What the outside world can see about your firm.

DNS · Web Properties · IP Addresses

DIMENSION 4

Cloud App Assessment

Configuration review of Microsoft 365 and key cloud services — identifying misconfigurations and policy gaps that could expose data or create compliance issues.

Microsoft 365 · AI Tools · Cloud Services

THE PROCESS & THE REPORT

A structured engagement — designed to produce a report that stands up to scrutiny.

Every assessment engagement follows the same four-step process. The difference from a typical vulnerability scan: the firm gets a remediation window between the initial findings and the final report. What you hand to a regulator, home office, or cyber insurer reflects your firm's remediated posture — not a list of open issues.

01 **Initial Assessment**

FCI runs the tools — external and internal penetration testing, vulnerability scanning, endpoint checks, cloud configuration review — to validate the firm's current cyber posture across the assessment dimensions that were scoped. The firm provides access as needed; FCI performs the technical work. This is the baseline from which remediation will be measured.

02 **Findings & Draft Report**

FCI consolidates the results into a draft report with severity rankings and remediation recommendations. The firm sees exactly what was found — and what to do about it — before anything is finalized.

03 **Remediation Window**

The firm fixes and improves what the draft report surfaced. FCI can provide remediation help on request — scoped separately and not included in the assessment price. This is the stage that makes the final report clean.

04 **Second Assessment & Final Report**

FCI runs the same tools a second time against the remediated environment and delivers the final written report — formatted for direct submission to regulators, home offices, and cyber insurance carriers. The report reflects current posture, not the list of issues found during the first assessment.

What's in the final report. Every engagement produces a written report whose format and content depend on the dimensions assessed — always designed to be submitted directly to the audience that requested it.

Vulnerability Findings

Identified vulnerabilities ranked by severity, with remediation recommendations and confirmation of what was resolved during the remediation window.

Penetration Test Results

Detailed results of external and internal penetration testing — what was tested, what was found, and what was remediated before final delivery.

Configuration Review

Cloud and endpoint configuration findings with specific policy gaps identified — and verification of corrections applied before the final scan.

Executive Summary

A concise overview suitable for firm leadership, compliance officers, and non-technical stakeholders — framing the firm's remediated posture, not a list of open issues.

WHO NEEDS THIS

Assessments fit into every stage of a firm's security lifecycle.

Security assessments are not a one-time event. Firms need them at different moments — and for different reasons. FCI works with firms across all three markets, whether they're proactively building their posture or responding to something that's already happened.

Exam Preparation

Your next FINRA, SEC, or state exam is coming. You need current vulnerability scans, penetration test results, and evidence your controls are in place.

Cyber Insurance Renewal

Your carrier is asking about your security posture. FCI's assessment provides the documentation they need to see.

Home Office Requirements

Your broker-dealer or insurance carrier home office is requiring branch offices to demonstrate compliance. FCI provides the evidence.

Post-Incident Readiness

After an incident, regulators ask for your last vulnerability assessment and pen test. If those don't exist or are outdated — it's an immediate credibility problem.

New Firm Onboarding

You're joining a new home office or switching compliance oversight. The assessment gives you a baseline that demonstrates due diligence from day one.

Annual Security Review

Best practice calls for regular assessment. FCI provides it on a cadence that matches your regulatory cycle.

FINRA | SEC | NAIC | State Regulators | Cyber Insurance Carriers

GETTING STARTED

Start with the gap analysis — it costs nothing and commits you to nothing.

The gap analysis is a 30-minute call with FCI. No preparation required on the firm's part. FCI will walk through what controls are in place, what's missing, and what your next exam, renewal, or home office requirement will likely ask for. From there, the firm decides what, if anything, to do next.

GAP ANALYSIS

Free — 30 Minutes — No Commitment

A clear picture of where you stand today — what controls are in place, what's missing, and what your next exam or renewal will require. This call is the starting point for every assessment engagement and comes with no obligation.

FORMAT	DURATION
Video call	30 minutes
COST	**OUTCOME**
Free	Gap analysis + scoped recommendations

> "Most firms don't know what their examiner will ask for until the examiner asks. The gap analysis gives you that answer in 30 minutes — before the clock starts."

Ready to find out where your firm stands?

FCI works with broker-dealers and branch offices, insurance carriers and agencies, and RIAs. The gap analysis is free — call to schedule.

PHONE

973-227-8878

WEB

fcicyber.com