hermetic networks

FTC Safeguards Rule Compliance for Financial Services Firms



FY2026

A Practical Guide for CPA Firms, RIAs, Broker-Dealers, and Other Financial Institutions

What is the FTC Safeguards Rule?

The FTC Safeguards Rule (16 CFR § 314) is a federal regulation that requires financial institutions to develop, implement, and maintain a comprehensive information security program to protect customer information. Originally enacted under the Gramm-Leach-Bliley Act (GLBA), the Rule was significantly updated in 2023 to reflect modern cybersecurity threats and expectations. The Rule applies to a broad range of financial services providers, including:

- CPA firms that provide tax preparation or financial planning
- Registered Investment Advisors (RIAs)
- Mortgage brokers and lenders
- Credit counselors and debt collectors
- Any business that receives customer information from a financial institution

What Does Compliance Actually Mean?

For CPA firms, the FTC Rule acts as the mandatory framework for meeting the security requirements of IRS Publication 4557 (Safeguarding Taxpayer Data). Both regulations require your firm to develop a program to protect sensitive client information. The 2023 updates to the FTC Rule made this compliance far more prescriptive, moving beyond general guidelines to specific, enforceable requirements. You must now:

Designate a Qualified Individual: Appoint someone responsible for overseeing your information security program. This person must have the authority and resources to implement safeguards.

Conduct Regular Risk Assessments: Perform an annual written risk assessment that identifies reasonably foreseeable risks to customer information, evaluates the likelihood and potential damage of threats, and assesses the effectiveness of your current safeguards.

Design and Implement Safeguards: Deploy controls based on your risk assessment, including:

- MFA for all systems accessing customer information
- Encryption of data at rest and in transit
- Access controls and least-privilege principles
- Change management procedures

What Happens if You're Not Compliant?

The FTC has enforcement authority and can impose significant penalties for non-compliance:

- Civil penalties exceeding $50,000 per violation, adjusted annually for inflation
- Consent decrees requiring third-party audits for 20 years
- Reputational damage from public enforcement actions
- State-level enforcement through attorneys general
- Increased liability in the event of a data breach

Beyond regulatory risk, non-compliance creates operational vulnerabilities. Firms without proper safeguards face higher risks of ransomware attacks, data breaches, business disruption, and client loss.

Monitor and Test Your Program: Continuously monitor the effectiveness of your safeguards and conduct regular testing, including:

- Vulnerability assessments every six months (minimum)
- Annual penetration testing
- Security monitoring and incident detection

Manage Service Providers: Maintain an up-to-date inventory of service providers that handle customer information, conduct due diligence on their security practices, and ensure contracts require appropriate safeguards.

Train Your Team: Provide regular security awareness training to all personnel, tailored to their roles and responsibilities.

Maintain a Written Information Security Program (WISP): Document your entire security program in a formal WISP, approved by your board or a senior officer and reviewed annually.

Report to Leadership: Provide at least annual written reports to your board or senior management on the status of your information security program, including material changes, test results, and security events.

Why It Matters

For a CPA firm, RIA, or broker-dealer, the Safeguards Rule turned security from an IT preference into a legal obligation. Client tax records, account numbers, and Social Security numbers are the raw material of your practice, and the federal government now holds your firm—not your software vendors—responsible for protecting them. Firms that treat compliance as paperwork usually discover the gap at the worst possible moment.





01

Cyber insurance requirements have evolved.

Insurers now demand evidence of multi-factor authentication, endpoint detection, documented incident response plans, and regular risk assessments before issuing or renewing policies.

02

Regulatory enforcement is intensifying.

The FTC Safeguards Rule, IRS Publication 4557, and a growing list of state privacy laws now hold firm owners directly accountable for protecting client information, with no exemption for small practices.

What's Required and When?

The FTC Safeguards Rule establishes a clear compliance calendar that financial institutions must follow to maintain their information security program. Here's what's required and when:

Requirement	Frequency	Trigger Events
Risk Assessment	Annually	Material changes to systems, operations, or business model.
Penetration Testing	Annually	Major infrastructure changes, cloud migrations, new critical systems
Vulnerability Assessments	Every 6 Months	New systems, network changes, vendor integrations
Security Monitoring Review	Quarterly	Security alerts, suspicious activity, vendor notifications
Policy Review & Updates	Annually	Regulatory changes, operational changes, audit findings
Service Provider Due Diligence	Annually	New vendors, contract renewals, security incidents
Security Awareness Training	Annually	New hires, role changes, after security incidents
Board / Management Reporting	Annually	Material security events, program changes, test results

Frequently Asked Questions

01 Does this apply to my firm if we're "small" or don't think we handle sensitive data?

Yes. If you're a CPA firm preparing tax returns, you handle Social Security numbers, financial account information, and income details—all considered customer information under GLBA. Size doesn't matter; the Rule applies based on the nature of services provided, not firm size.

02 We use cloud services like Microsoft 365 and QuickBooks Online. Doesn't that make us compliant?

Not automatically. While cloud providers offer strong security features, you are still responsible for configuring those tools correctly, enforcing MFA, managing access, conducting risk assessments, and documenting your program. The Safeguards Rule requires you to verify and validate your security posture—not just assume your vendors handle it.

03 Our CPA software vendor says they handle security. Isn't that enough?

This is one of the most common—and most dangerous—misconceptions about FTC Safeguards Rule compliance. The reality is that your software vendor's security practices do not exempt you from compliance obligations. The FTC Safeguards Rule places legal responsibility directly on your firm as the financial institution, not on your technology vendors.

04 How much should compliance cost?

It depends on your firm's size, complexity, and current security posture. Initial implementation (risk assessment, WISP creation, policy development, first pen test) typically ranges from $8,000–$25,000. Ongoing compliance (annual testing, monitoring, evidence collection, policy updates) runs $500–$2,500/month depending on service levels. However, the cost of *non-compliance*—regulatory fines, breach response, client loss, downtime—is far higher.

05 Can we phase in compliance over multiple years?

Short answer: No—all requirements took effect on June 9, 2023 and must be met now.
The longer answer: You can phase in improvements, but you cannot defer requirements. Your first-year compliance program may rely more on manual processes—and that's acceptable. But you must meet all requirements from day one.

06 What is penetration testing, and why is it required annually?

Penetration testing (or "pen testing") is a simulated cyberattack conducted by qualified security professionals to identify exploitable vulnerabilities in your systems, applications, and network infrastructure. Unlike vulnerability scans that simply identify potential weaknesses, penetration tests actively attempt to exploit those weaknesses to determine what an attacker could actually access. The Rule gives you a choice: continuous monitoring of your systems, or annual penetration testing plus vulnerability assessments every six months. Most small firms choose the testing path.

07 What happens during an FTC investigation or audit?

FTC investigations are typically triggered by several factors rather than random selection. This could include consumer complaints, data breaches, referrals from other agencies, media reports, or whistleblowers. The FTC generally doesn't conduct random audits of compliance - investigations are reactive. They typically begin with a Civil Investigative Demand (CID) requiring you to produce documents and answer questions relating to your security practices.

Quick Reality Check

Software alone doesn't make a business compliant, and neither do policies on paper. Compliance comes from following the policies in practice and being able to show evidence. Before assuming you're fully covered, it's worth comparing the most common assumptions with what the law actually requires.



Risk Assessment

The Myth: "We did a penetration test last year, so we know our risks."

The Mandate: A penetration test is not a Risk Assessment. The FTC Rule requires a written Risk Assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information.

Incident Response Plan (IRP)



The Myth: "If we get hacked, we'll just call the IT guy!"

The Mandate: You must have a written Incident Response Plan designed to promptly respond to and recover from a security event. It must explicitly define roles, responsibilities, decision-making authority, and internal/external communications. It's a standalone legal requirement, not a general IT function.



Data Disposal

The Myth: "We keep everything just in case."

The Mandate: The Rule requires the secure disposal of customer information no later than two years after the last date the information was used, unless there is a legitimate business need or legal requirement to retain it. Holding onto old client data "just because" is now a regulatory violation.

Multi-Factor Authentication (MFA)

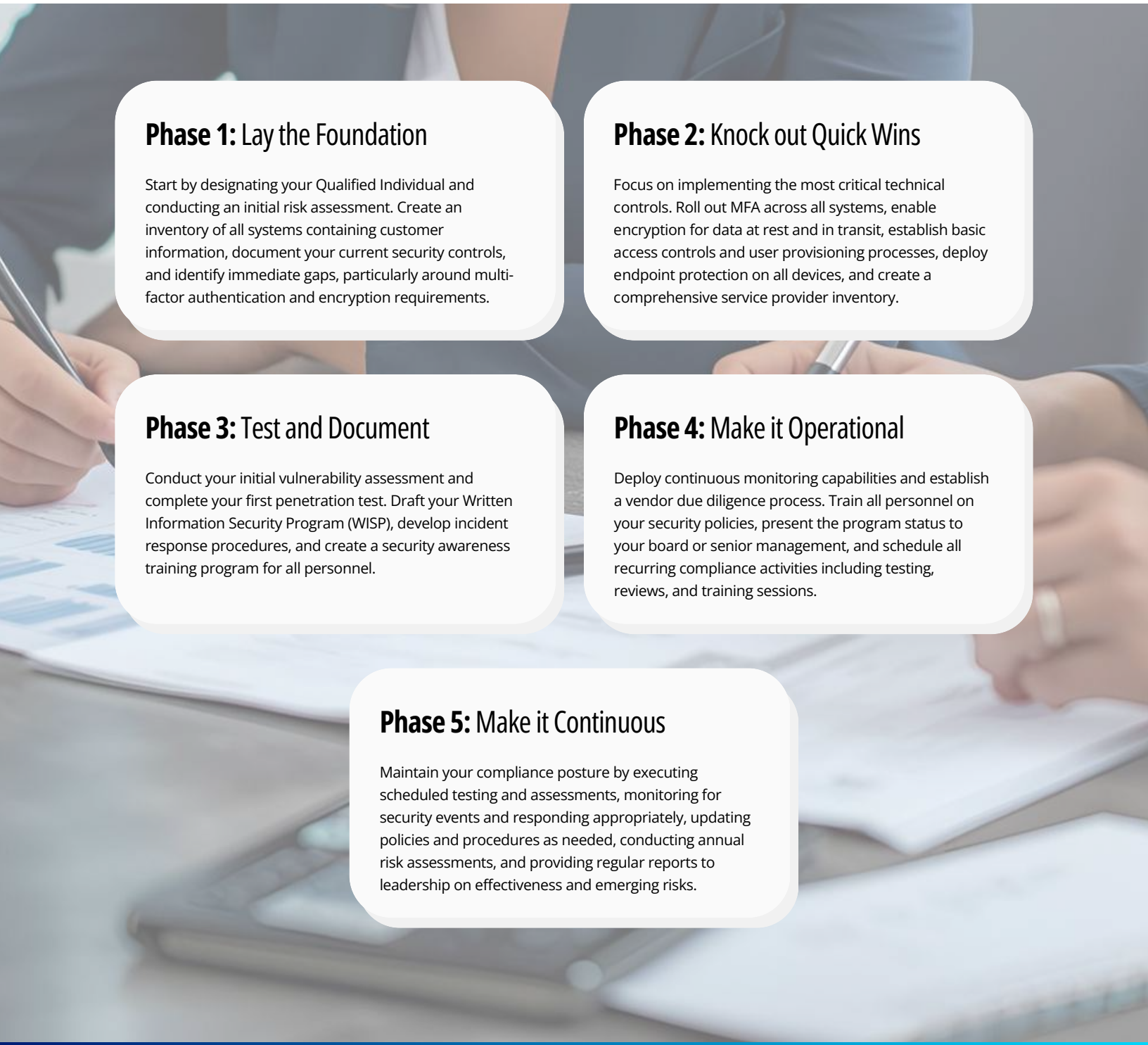


The Myth: "We have 2FA turned on for our remote users, so we're good."

The Mandate: The Rule requires MFA for any individual accessing customer information on your system, not just remote workers. Yes, this applies to VPN, but any software containing customer data, too. If your staff logs into tax software at their desks without MFA, we have some work to do.

How to Get Started

If you're just beginning your compliance journey, here's a practical roadmap for your first twelve months.



Phase 1: Lay the Foundation

Start by designating your Qualified Individual and conducting an initial risk assessment. Create an inventory of all systems containing customer information, document your current security controls, and identify immediate gaps, particularly around multi-factor authentication and encryption requirements.

Phase 2: Knock out Quick Wins

Focus on implementing the most critical technical controls. Roll out MFA across all systems, enable encryption for data at rest and in transit, establish basic access controls and user provisioning processes, deploy endpoint protection on all devices, and create a comprehensive service provider inventory.

Phase 3: Test and Document

Conduct your initial vulnerability assessment and complete your first penetration test. Draft your Written Information Security Program (WISP), develop incident response procedures, and create a security awareness training program for all personnel.

Phase 4: Make it Operational

Deploy continuous monitoring capabilities and establish a vendor due diligence process. Train all personnel on your security policies, present the program status to your board or senior management, and schedule all recurring compliance activities including testing, reviews, and training sessions.

Phase 5: Make it Continuous

Maintain your compliance posture by executing scheduled testing and assessments, monitoring for security events and responding appropriately, updating policies and procedures as needed, conducting annual risk assessments, and providing regular reports to leadership on effectiveness and emerging risks.

How Hermetic Can Help

Compliance is not a tool you can buy. It's a system you have to build. And regulators evaluate the system—not the parts. That's why Hermetic Networks built a complete Managed Compliance Program specifically for small and mid-sized CPA firms.

The Hermetic Managed Compliance Program

A complete, regulator-aligned security framework—built for real firms, not enterprises.

We replace uncertainty with clarity, scattered tools with a unified framework, and replace guesswork with documented, repeatable controls, including:

- A complete Written Information Security Program (WISP) designed to satisfy auditors
- Every required policy under the FTC Safeguards Rule
- Every safeguard required under IRS Publication 4557
- An audit-ready Incident Response Plan, including the IRS 24-hour reporting rule
- Continuous monitoring, vulnerability scanning, and oversight
- Evidence trails that satisfy cyber insurance and legal requirements

This program gives your firm the confidence, documentation, and operational structure needed to pass an audit, survive an incident, and satisfy insurance claims.

What Your Firm Receives

GOVERNANCE

- Written Information Security Program (WISP)
- Integrated IRS 4557 / FTI Safeguards
- Annual Risk Assessment with documented findings and remediation priorities
- Employee Security Training & Acknowledgment Tracking
- Policy Governance & Annual Review
- Qualified Individual Support for oversight and reporting

Outcome: Leadership can prove the firm is governing security with intention and evidence — exactly what regulators want to see.

OPERATIONAL SECURITY

- Compliance Policy Pack (all required FTC/IRS policies)
- Incident Response Policy defining authority and escalation
- Incident Response Plan (IRP) ready for auditors and insurance carriers
- Secure Access & Device Standards for every workstation
- Quarterly Access Reviews to enforce least-privilege
- Configuration Baseline Enforcement across devices
- Continuous Vulnerability Scanning to identify risks early

Outcome: You eliminate the single biggest risk in small firms: inconsistent or undocumented day-to-day behavior.

MONITORING & OVERSIGHT

- Logging & Monitoring of critical device events
- Incident Detection & Escalation Procedures
- Vendor Oversight & Safeguards Validation
- Monthly Compliance Scorecard
- Annual Program Review & WISP Refresh

Outcome: Your firm maintains a continuous, provable security posture instead of a once-a-year checklist.

What are the Benefits?

1. It removes the burden from leadership.
The Qualified Individual no longer has to manage logging, vendor oversight, policy updates, risk assessments, training, or evidence gathering. We handle the operational workload while leadership maintains high-level oversight.

2. It satisfies regulators and insurance carriers.
The program produces all required artifacts—WISP, Risk Assessment, IR Plan, policy acknowledgments, and access/log review evidence—so the firm is fully prepared for audits, renewals, or incidents.

3. It's built for small firms but aligned to enterprise standards.
Designed for 5–50-user CPA practices, the program maps directly to NIST, CIS, FTC Safeguards Rule, IRS 4557, and cyber insurance requirements, delivering enterprise-grade compliance without enterprise overhead.

4. It creates defensibility.
In a breach or audit, firms must show documented policies, evidence of implementation, and continuous oversight. This program provides all three, giving your firm a defensible position when it matters most.

What Compliance Costs

Below is what the work actually costs. One-time projects establish your baseline compliance; recurring services keep it current between audits. Every engagement is scoped to your firm's size and systems, so treat these figures as planning ranges rather than quotes.

One-Time Compliance Projects

Foundational work required to establish baseline FTC/GLBA compliance.

Service	Description	Pricing
Risk Assessment	Written SRA/GLBA RA with likelihood/impact scoring, safeguards mapping, remediation roadmap, and complete data inventory.	$5,000 - $8,000
WISP Creation	Full GLBA/FTC-compliant Written Information Security Program with basic policies, IR plan, vendor oversight, and control mapping.	$2,000
Penetration Testing	External only: attack surface + exploitation validation. Internal+External: full lateral movement analysis.	Quoted per engagement
Vulnerability Assessment	Internal & external vulnerability scans, findings, remediation guidance, and audit documentation.	$1,000 - $5,000
Policy Development	Administrative and technical security policies (AUP, Access Control, IR, Encryption, Vendor Management, etc.).	$250–$750 /policy

Recurring Operational Compliance Services

Ongoing MSP operational services that maintain compliance posture.

Service	Description	Pricing
Continuous Vulnerability Scanning	Full network scanning, findings review, remediation ticketing, and compliance summaries.	$500 / mo.
Evidence Collection & Management	Quarterly monitoring review, evidence capture, vendor list updates, data inventory updates, audit-ready packaging.	$1,000 / mo.
Fully Managed Compliance	Includes all one-time and recurring services listed above.	Monthly Base + Per User Fee

vCIO

A Virtual CIO (vCIO) is your firm's technology strategist. Most firms this size have no one whose job is to look twelve months ahead at renewals, capacity, and spend, so those decisions get made under pressure—usually in the middle of your busiest season. The vCIO builds the roadmap and the budget, then holds your vendors to both.

Core Functions

- IT strategy and roadmap
- Annual budgeting and lifecycle planning
- Cloud and infrastructure modernization
- Vendor and contract management
- Governance and policy development
- Business continuity and disaster recovery planning

vCIO Partnerships starting at $1,500 / mo.

vCISO

A Virtual CISO (vCISO) can serve as the Qualified Individual the Safeguards Rule requires you to designate, without the cost of a full-time security hire. Your firm still retains responsibility and names a senior staff member to oversee the role, but the vCISO owns the work: risk assessments, the WISP, vendor oversight, and the annual report to leadership.

Core Functions

- Security risk assessments
- Written Information Security Program (WISP)
- Compliance readiness (NIST, CIS, ISO, GLBA)
- Incident response and testing
- Vendor risk management
- Employee security awareness oversight

vCISO Partnerships starting at $2,500 / mo.

Next step: a no-charge scoping call. We will review your current safeguards against the Rule, show you where the gaps are, and give you a written scope and price. Start at hermeticnetworks.com.