

FTC Safeguards + IRS Readiness Checklist

ASTEROID IT

For CPA firms, tax preparers, and accounting practices

If your firm prepares tax returns or provides financial advice to individuals, federal law treats you as a financial institution. The FTC Safeguards Rule (16 CFR Part 314) names "an accountant or other tax preparation service" directly. This checklist covers what the rule actually requires, what the IRS requires on top of it, and which items your firm is exempt from based on size.

Before you start: which parts apply to your firm

Answer these five first	Your answer
Does your firm prepare tax returns, give tax advice, run payroll, or provide financial planning for individuals? Yes means the Safeguards Rule almost certainly applies to your firm, at any size.	Yes / No
Does your firm maintain customer information on 5,000 or more consumers? Under 5,000 exempts you from four requirements (16 CFR 314.6). Count everyone whose data you hold, not just active clients. If unsure, answer Yes.	Yes / No / Not sure
Is your firm an Authorized IRS e-file Provider (do you hold an EFIN)? Adds IRS Publication 1345 obligations, including a next-business-day incident report.	Yes / No
Do clients submit taxpayer information through a website your firm operates? Online Providers must contract a third party for weekly external vulnerability scans. A portal hosted by your tax software vendor usually does not make you an Online Provider. Check with your vendor.	Yes / No
Do you have clients who live outside Arizona? Breach notice obligations follow where your clients live, not where your office is.	Yes / No

If you hold information on fewer than 5,000 consumers, Part B does not apply to you. 16 CFR 314.6 exempts firms below that threshold from the written risk assessment, the monitoring and penetration testing requirement, the written incident response plan, and the annual report. You must still base your program on a risk assessment, and everything in Parts A, C and D applies in full at any size. Count everyone whose information you hold, not just active clients.

Items marked **CRITICAL** have no size exemption and are the ones that sink an insurance application or a client security review. Work those first.

Part A | Core program

Required of every covered firm regardless of size. There is no small-firm exemption for anything in this section.

Requirement	Reference	Y	P	N
A1 A Qualified Individual is named in writing to run the security program One named person is accountable. They can work for you or for your IT provider.	314.4(a) CRITICAL			

Requirement	Reference	Y	P	N
A2 If that person works for an outside provider, a senior person inside the firm is named to oversee them Outsourcing the role does not move the legal responsibility. The firm keeps it, and must designate someone internally to direct and oversee the provider.	314.4(a)(1)-(3) CRITICAL			
A3 Access to client data is limited to the people who need it, and is reviewed periodically Least privilege, applied to tax software, file shares, email, and the document portal.	314.4(c)(1)			
A4 You keep a current inventory of the data, devices, systems, and locations holding client information You cannot protect what you have not listed. This includes laptops at home, old servers, and archived backups.	314.4(c)(2) CRITICAL			
A5 Client information is encrypted at rest and in transit If encryption is not feasible somewhere, the Qualified Individual must approve compensating controls in writing. A verbal decision does not satisfy the rule.	314.4(c)(3) CRITICAL			
A6 The security of outside software you rely on has been evaluated Tax software, the client portal, cloud storage, e-signature tools. Any in-house built tool needs secure development practices.	314.4(c)(4)			
A7 MFA is on for every person accessing any system that holds client information The rule covers any individual accessing any information system, not just staff email. That includes partners, seasonal preparers, bookkeepers, and your IT vendor. Anything less requires written QI approval of equivalent controls.	314.4(c)(5) CRITICAL			
A8 Client information is disposed of no later than two years after its last use Unless you have a business or legal reason to keep it, documented. Most firms are holding 10+ years of returns with no written basis.	314.4(c)(6)(i) CRITICAL			
A9 Your retention policy gets reviewed so you stop holding data you no longer need A periodic review is required, not just a policy written once.	314.4(c)(6)(ii)			
A10 You follow a documented change management process Who approves a new application, a firewall change, or a new cloud service, and how it gets recorded.	314.4(c)(7)			
A11 Activity of authorized users is logged and monitored so unauthorized access can be detected This is the item that decides whether you can rebut the breach presumption in Part C. Without logs you generally cannot.	314.4(c)(8) CRITICAL			

Requirement	Reference	Y	P	N
A12 Key controls are regularly tested or otherwise monitored for effectiveness Applies to every firm. The heavier pen-test requirement in Part B does not.	314.4(d)(1)			
A13 All staff receive security awareness training, refreshed as new risks appear Training must reflect the risks you actually identified, not a generic annual video.	314.4(e)(1) CRITICAL			
A14 Qualified security personnel, in-house or through a provider, keep current on threats The rule expects someone competent and current, and expects you to verify that they are.	314.4(e)(2)-(4)			
A15 Vendors who touch client data are under written agreements requiring safeguards, and are reassessed periodically Selection, contract language, and ongoing review are three separate obligations. A standard terms-of-service click-through does not satisfy this.	314.4(f) CRITICAL			
A16 The program is updated after incidents, test results, or material changes to the firm New office, new cloud platform, a merger, or a near miss should all trigger a revision.	314.4(g)			

Part B | Additional requirements at 5,000 or more consumers

16 CFR 314.6 exempts firms holding information on fewer than 5,000 consumers from these four. You are still required to base your program on a risk assessment, it simply does not have to meet the written specification below.

Requirement	Reference	Y	P	N
B1 A written risk assessment with criteria for evaluating and categorizing risks It must also state how each identified risk will be mitigated or accepted, and be redone periodically.	314.4(b)(1)			
B2 Continuous monitoring, or annual penetration testing plus vulnerability assessments every six months Antivirus alone is not this. It is one or the other: real continuous monitoring, or the testing cadence.	314.4(d)(2)			
B3 A written incident response plan It must cover goals, internal process, roles and decision authority, internal and external communications, remediation, documentation, and post-incident revision.	314.4(h)			
B4 The Qualified Individual reports in writing at least annually to the partners or a senior officer Covering program status, risk decisions, vendor arrangements, test results, and any security events. An informal annual conversation does not meet this.	314.4(i)			

Part C | When something happens: the clocks

Most firms discover these deadlines during the incident. That is the worst time to read them.

Requirement	Reference	Y	P	N
C1 You know a breach involving 500 or more consumers must be reported to the FTC within 30 days of discovery Filed on the FTC's electronic form. The report becomes public.	314.4(j)(1) CRITICAL			
C2 You understand that unauthorized access is presumed to be unauthorized acquisition The presumption stands unless you hold reliable evidence that acquisition did not and could not reasonably have occurred. Logs are that evidence.	314.2(m)			
C3 You know the 30-day clock starts when any employee or agent learns of it Not when the partners are told. Staff need to know to escalate immediately.	314.4(j)(2)			
C4 Security incidents are reported to the IRS no later than the next business day after confirmation [e-file providers] This is far tighter than the FTC's 30 days and it is the deadline most firms miss. EROs contact their IRS Stakeholder Liaison.	IRS Pub 1345 CRITICAL			
C5 You know which states' breach laws apply, based on where your clients live Arizona's statute does not apply to persons covered by GLBA Title V (A.R.S. 18-552(N)), so an Arizona firm is often out from under it. Other states differ, and a handful run a 30-day clock.	A.R.S. 18-552(N)			
C6 Incident contacts are written down and reachable outside business hours Cyber insurer, counsel, IT provider, IRS Stakeholder Liaison. Tax season incidents do not wait for Monday.	314.4(h) / practice			

Part D | IRS and tax-specific requirements

The FTC writes the rule, but the IRS holds what you actually care about: your PTIN and your EFIN. Nothing in this section has a size exemption.

Requirement	Reference	Y	P	N
D1 You have a WISP that follows IRS Pub 4557 and Pub 5708 and names your real systems, staff, vendors, and locations The Pub 5708 sample is a starting structure, not a finished plan. A template with the blanks unfilled is the most common finding.	IRS Pub 4557 / 5708 CRITICAL			

Requirement	Reference	Y	P	N
D2 The WISP is reviewed before each PTIN renewal Form W-12 Line 11 asks you to acknowledge the legal requirement to maintain a WISP. It does not mean the IRS reviewed or approved yours.	Form W-12, Line 11 CRITICAL			
D3 Your EFIN is protected and your IRS return count is checked against what you actually filed [e-file providers] A mismatch is often the first visible sign that your credentials are being used by someone else.	IRS Pub 1345			
D4 A third party runs weekly external network vulnerability scans, per PCI DSS requirements [Online Providers only] This applies to Online Providers, meaning firms collecting taxpayer information through their own website. It does not apply to every ERO.	IRS Pub 1345			
D5 You obtain written client consent before any disclosure or use of return information that requires it Consents have specific form and content requirements. Using return data for marketing or a side service without one is the classic violation.	IRC 7216 / 301.7216-3 CRITICAL			
D6 Every vendor who can reach return information has received written notice of the IRC 7216 and 6713 penalties Most firms have never done this. If your IT provider, software vendor, or offshore preparer can see return information and did not get that written notice, the disclosure is impermissible even though the vendor is legitimate.	Treas. Reg. 301.7216-2(d) CRITICAL			
D7 No return information goes outside the United States without the specific consent the regulations require Relevant if you use offshore preparation, offshore bookkeeping, or a support desk located abroad.	301.7216-3			

How to score yourself

Count only the items that apply to your firm. Give yourself full credit for Yes, half for Partial, nothing for No. Then check your critical items separately, because a single open critical gap outranks a good overall percentage.

Where you land	What it means
Any critical gap open	Treat this as an active finding. Critical items have no size exemption, and a single one open is enough to fail a client security review or an insurance application.
Under 70% ready	The program does not yet exist in a form you could show a regulator, an insurer, or a client's auditor.
70% to 89% ready	The controls are largely in place but the documentation and evidence behind them are thin. This is where most firms sit.

Where you land	What it means
90% or better	Strong position. The remaining work is usually evidence and cadence rather than new technology.

A note on penalties, because the internet is loud about this. The FTC's maximum civil penalty is \$53,088 per violation and is unchanged for 2026. We are not aware of any FTC enforcement action against a small CPA or tax firm. The realistic exposure for a firm your size is your PTIN attestation, your EFIN, a denied cyber insurance claim, and the cost of notifying clients. Those are reason enough.

What to do with your results

Fix the critical gaps first. Every critical item applies to your firm regardless of size, and most can be closed in days rather than months.

If you want a second set of eyes, Asteroid IT offers a free Safeguards readiness review for CPA and tax firms. We go through your answers, tell you which gaps actually matter for a firm your size, and give you the remediation order. No obligation, and we will tell you if you do not need us.

Asteroid IT

support@asteroidit.com · 480-937-7021

Your clients trust you with their most sensitive data. We help you keep that trust.

This checklist is general information, not legal advice. Citations are to 16 CFR Part 314 as amended through May 13, 2024, and to current IRS guidance. Your obligations depend on your facts. Confirm anything consequential with your counsel.

© Asteroid IT. Share this freely with anyone who needs it.