ALL BUSINESS TECHNOLOGIES

SAMPLE REPORT · FICTIONAL FIRM

FTC SAFEGUARDS RULE · IRS PUB 4557 · IRS PUB 5708

Safeguards Readiness Report

Harborview Tax & Accounting

Prepared for Alex Morgan · 6–15 people · October 19, 2026
alex@example.com · (508) 555-0100

Report ID 5A3E1C7B

46
OUT OF 100

HIGH RISK

SAMPLE

CONTENTS

01 Executive summary 2
02 Scorecard 3
03 30/60/90-day action plan 4
04 Gap detail 6
05 Evidence binder 13
06 Full answer summary 14
07 Next steps, sources & disclaimer 15

Provided by All Business Technologies. Not affiliated with or endorsed by the FTC or IRS.

01 · EXECUTIVE SUMMARY

Where your firm stands

Based on Harborview Tax & Accounting's answers to 25 questions mapped to the FTC Safeguards Rule (16 CFR Part 314), IRS Publication 4557 and IRS Publication 5708, completed October 19, 2026.



At a glance

Significant gaps in required safeguards. Prioritize the critical items below.

7	8	10
In place	Partial	Gaps / not sure

30/60/90-day plan	**6 · 5 · 6 items by phase (+1 later)**
Evidence binder	**2 of 16 documents ready**
Gaps by priority	**2 critical · 10 high · 6 medium**

CRITICAL GAP

MFA, a written security program (WISP) and encryption are critical safeguards. While any of them is answered No or Not sure, the risk level cannot be Low and the score is capped at 84.

- **Encryption in transit** — §314.4(c)(3) · Your answer: Not sure

Fix first

01 Data in transit not encrypted — §314.4(c)(3)
Tax returns and ID documents sent as plain email attachments can be intercepted or forwarded. A secure portal or encrypted email keeps them private.

02 No written incident response plan — §314.4(h)
The first hours of a breach decide how bad it gets. A plan means people know who to call and what to do, instead of improvising.

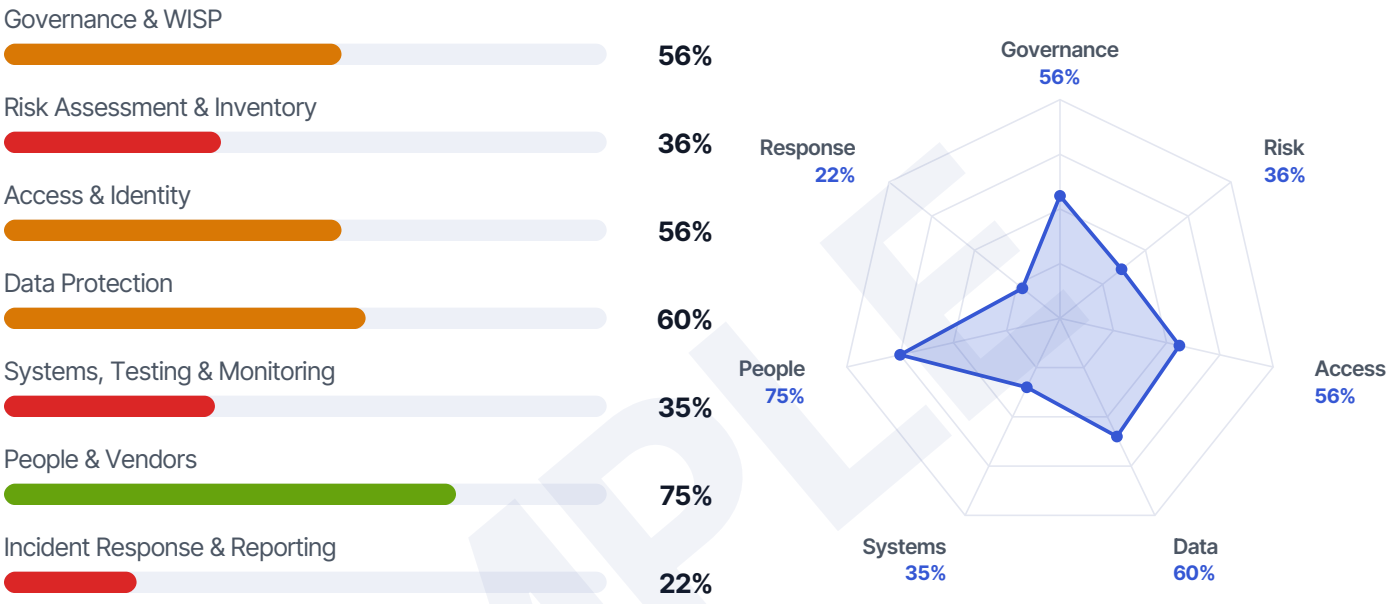
03 No annual written security report to leadership — §314.4(i)
A yearly written report keeps the partners informed about risk and shows that leadership is overseeing the program, not just IT.

SAMPLE

02 · SCORECARD

Scores by control area

Weighted scores for each of the seven control areas.



HOW YOUR SCORE WORKS

Weights	Each question is weighted by impact: core and critical controls count 3, high-impact controls 2, standard controls 1.
Answers	Yes earns full credit, Partially earns half, and No or Not sure earn zero. Not sure counts as a gap because a control you cannot verify cannot be relied on.
Critical-control cap	If MFA, the written security program (WISP), or encryption at rest or in transit is No or Not sure, the score is capped at 84 and the risk level cannot be Low.
Risk levels	85 to 100 is Low, 65 to 84 Moderate, 40 to 64 High, below 40 Critical. ABT set these weights and bands; they are not defined by the FTC or IRS.
Small firms	With customer information on fewer than 5,000 consumers, 16 CFR 314.6 exempts four elements: the written risk assessment, pen testing and vulnerability scans, the written incident response plan and the annual report. They are shown as "Best practice at your size" and left out of the score. Everything else still applies.

WHAT YOU'RE DOING WELL

Qualified Individual · Unique logins & least privilege · Encryption at rest · Protected backups · Endpoint protection & updates · Security awareness training · EFIN/PTIN monitoring

SAMPLE

03 · 30/60/90-DAY ACTION PLAN

30/60/90-day action plan

Critical gaps and quick wins first, then larger projects, then the documents and policies that tie it together. Each item shows the effort it usually takes.

01 First 30 days — Critical gaps and quick wins — 6 items

Encryption in transit CRITICAL §314.4(c)(3)
Use a secure client portal or encrypted email instead of plain attachments.
Quick win · Typically needs an IT partner

Incident response plan §314.4(h)
Write an incident response plan covering all seven areas in §314.4(h).
Documentation · Typically needs an IT partner

Periodic access reviews §314.4(c)(1)
Review user accounts and permissions at least quarterly, and record the date and outcome.
Quick win · DIY-friendly

FTC breach notice procedure §314.4(j)
Add the FTC 30-day notification step and the FTC online form link to your incident procedures.
Quick win · DIY-friendly

IRS data-theft reporting Pub 4557
Look up your IRS Stakeholder Liaison and state agency contacts and record them in your WISP or incident procedures.
Quick win · DIY-friendly

Multi-factor authentication (MFA) §314.4(c)(5)
Turn on MFA for email, tax and accounting software, client portals, cloud storage and remote access.
Quick win · Typically needs an IT partner

02 Days 31–60 — Larger projects — 5 items

Activity logging §314.4(c)(8)
Turn on audit logging in Microsoft 365 or Google Workspace, your tax software and file storage.
Project · Typically needs an IT partner

SAMPLE

Pen testing & vulnerability scans §314.4(d)(2)
Deploy effective continuous monitoring, or schedule vulnerability assessments at least every six months and after major changes.
Project · Typically needs an IT partner

Risk assessment §314.4(b)
List the threats to client data: phishing, ransomware, lost laptops, insiders and vendors.
Project · Typically needs an IT partner

Data & asset inventory §314.4(c)(2)
List every place client data lives: tax software, portals, email, file shares, cloud storage and paper files.
Project · Typically needs an IT partner

Safeguard testing & monitoring §314.4(d)(1)
Set a regular schedule to confirm key controls are working: MFA, encryption, backups, updates and security alerts.
Project · Typically needs an IT partner

03 Days 61–90 Documentation and policies — 6 items

Annual report to leadership §314.4(i)
Schedule a yearly written report from your Qualified Individual to the partners or senior officer.
Documentation · DIY-friendly

Written risk assessment §314.4(b)(1)
Write down the criteria you use to rate risks and to judge whether your controls are adequate.
Documentation · Typically needs an IT partner

Written security plan (WISP) §314.3(a)
Draft a WISP sized to your firm, using IRS Publication 5708 as a starting template.
Documentation · DIY-friendly

Secure disposal & retention §314.4(c)(6)
Write a retention schedule that reflects your legal retention obligations.
Documentation · DIY-friendly

Change management §314.4(c)(7)
Require a short security review before adding or changing systems, software or network gear.
Documentation · DIY-friendly

SAMPLE

Vendor oversight §314.4(f)
Identify every vendor with access to client data (IT, software, cloud, shredding, payroll).
Documentation
DIY-friendly

+ **After 90 days** Remaining items 1 item

App security review §314.4(c)(4)
List every app that stores or transmits client data.
Documentation
DIY-friendly

04 · GAP DETAIL

Gaps and how to close them

Every gap from your answers, ordered by priority and impact, with why it matters and what to do.

01 **Data in transit not encrypted** CRITICAL

Encryption in transit · Your answer: Not sure, needs verification · §314.4(c)(3)

WHY IT MATTERS

Tax returns and ID documents sent as plain email attachments can be intercepted or forwarded. A secure portal or encrypted email keeps them private.

WHAT TO DO

- Use a secure client portal or encrypted email instead of plain attachments.
- Make sure remote access and file transfers use encrypted connections.
- Document any QI-approved compensating control where encryption is infeasible.

Quick win | Typically needs an IT partner

Sources: 16 CFR 314.4, IRS Pub 4557

SAMPLE

02 **No written incident response plan** — CRITICAL

Incident response plan · Your answer: Not in place · §314.4(h)

WHY IT MATTERS

The first hours of a breach decide how bad it gets. A plan means people know who to call and what to do, instead of improvising.

WHAT TO DO

- Write an incident response plan covering all seven areas in §314.4(h).
- List who to call: IT/security, cyber insurer, legal counsel, IRS Stakeholder Liaison and state agencies.
- Run a tabletop exercise each year and update the plan afterwards.

Documentation | Typically needs an IT partner

Sources: 16 CFR 314.4, 16 CFR 314.6, IRS Pub 5708

03 **No annual written security report to leadership** — HIGH

Annual report to leadership · Your answer: Not in place · §314.4(i)

WHY IT MATTERS

A yearly written report keeps the partners informed about risk and shows that leadership is overseeing the program, not just IT.

WHAT TO DO

- Schedule a yearly written report from your Qualified Individual to the partners or senior officer.
- Cover program status, risk decisions, vendors, test results, incidents and recommendations.
- Keep signed copies with your WISP.

Documentation | DIY-friendly

Sources: 16 CFR 314.4, 16 CFR 314.6

04 **Risk assessment not documented** — HIGH

Written risk assessment · Your answer: Not in place · §314.4(b)(1)

WHY IT MATTERS

A written assessment proves you did the work and lets you show how your decisions were made. Insurers and examiners usually ask to see it.

WHAT TO DO

- Write down the criteria you use to rate risks and to judge whether your controls are adequate.
- Record, for each risk, whether you will mitigate or accept it, and how.
- Keep the dated document with your WISP.

Documentation | Typically needs an IT partner

Sources: 16 CFR 314.4, 16 CFR 314.6

SAMPLE

05 Access not reviewed regularly

HIGH

Periodic access reviews · Your answer: Not in place · §314.4(c)(1)

WHY IT MATTERS

Former staff and old vendor accounts that still work are an open door. A short, regular review closes it.

WHAT TO DO

- Review user accounts and permissions at least quarterly, and record the date and outcome.
- Remove access the day someone leaves, and adjust it when roles change.

Quick win | DIY-friendly

Sources: 16 CFR 314.4

06 No activity logging or monitoring

HIGH

Activity logging · Your answer: Not in place · §314.4(c)(8)

WHY IT MATTERS

Without logs you may not know a breach happened, or be able to tell which clients were affected when you must notify them.

WHAT TO DO

- Turn on audit logging in Microsoft 365 or Google Workspace, your tax software and file storage.
- Send alerts for suspicious sign-ins and mass file access or deletion.
- Assign someone to review alerts, and keep logs long enough to investigate.

Project | Typically needs an IT partner

Sources: 16 CFR 314.4, FTC Guide, IRS Pub 4557

07 No continuous monitoring, scans or pen testing

HIGH

Pen testing & vulnerability scans · Your answer: Not in place · §314.4(d)(2)

WHY IT MATTERS

Attackers scan for known weaknesses every day. Testing finds them first, so you fix them on your schedule instead of theirs.

WHAT TO DO

- Deploy effective continuous monitoring, or schedule vulnerability assessments at least every six months and after major changes.
- Commission an annual penetration test based on your risk assessment if you do not have continuous monitoring.
- Track findings to remediation and report results to leadership.

Project | Typically needs an IT partner

Sources: 16 CFR 314.4, 16 CFR 314.6

SAMPLE

08 No FTC breach-notification procedure

HIGH

FTC breach notice procedure · Your answer: Not in place · §314.4(j)

WHY IT MATTERS

The 30-day clock starts at discovery. Knowing the steps in advance avoids a missed federal deadline on top of a breach.

WHAT TO DO

- Add the FTC 30-day notification step and the FTC online form link to your incident procedures.
- Define who decides whether an event is a notification event and who files the report.
- Know roughly how many consumers' data you hold, so you can tell quickly whether the 500 threshold applies.

Quick win | DIY-friendly

Sources: 16 CFR 314.4, FTC Guide

09 IRS data-theft reporting not prepared

HIGH

IRS data-theft reporting · Your answer: Not sure, needs verification · Pub 4557

WHY IT MATTERS

Fast reporting lets the IRS and states watch for fraudulent returns in your clients' names, limiting the damage to them.

WHAT TO DO

- Look up your IRS Stakeholder Liaison and state agency contacts and record them in your WISP or incident procedures.
- Note when to involve law enforcement and your cyber insurer.

Quick win | DIY-friendly

Sources: IRS Pub 4557, IRS Pub 5708

10 Missing or outdated WISP

HIGH

Written security plan (WISP) · Your answer: Partially in place · §314.3(a)

WHY IT MATTERS

The written plan is the first document anyone will ask for after a breach. It applies to firms of every size, and without it every other safeguard is hard to prove.

WHAT TO DO

- Draft a WISP sized to your firm, using IRS Publication 5708 as a starting template.
- Store it where staff can read it, and keep an offsite or cloud copy.
- Review and update it whenever your people, systems or vendors change.

Documentation | DIY-friendly

Sources: 16 CFR 314.3, IRS Pub 5708, Form W-12 Instr.

SAMPLE

11 No periodic risk assessment

HIGH

Risk assessment · Your answer: Partially in place · §314.4(b)

WHY IT MATTERS

The risk assessment decides which safeguards you need. Skip it and you may spend money in the wrong places while real exposures stay open.

WHAT TO DO

- List the threats to client data: phishing, ransomware, lost laptops, insiders and vendors.
- Judge whether your current safeguards are enough for each, and decide how to reduce or accept each risk.
- Repeat the assessment at least yearly and after major changes.

Project | Typically needs an IT partner

Sources: 16 CFR 314.4, FTC Guide

12 MFA not enforced everywhere

HIGH

Multi-factor authentication (MFA) · Your answer: Partially in place · §314.4(c)(5)

WHY IT MATTERS

Stolen passwords are the most common way into email and tax software. MFA stops most of those attacks even when a password leaks.

WHAT TO DO

- Turn on MFA for email, tax and accounting software, client portals, cloud storage and remote access.
- Prefer authenticator apps or security keys over text messages.
- Document any exception, with the approved alternative control, in writing.

Quick win | Typically needs an IT partner

Sources: 16 CFR 314.4, FTC Guide, IRS Pub 4557

13 No data and asset inventory

MEDIUM

Data & asset inventory · Your answer: Partially in place · §314.4(c)(2)

WHY IT MATTERS

You cannot protect devices and data you do not know about. Forgotten laptops, old file shares and unused accounts are common ways in.

WHAT TO DO

- List every place client data lives: tax software, portals, email, file shares, cloud storage and paper files.
- List all devices, user accounts and vendors with access.
- Update the inventory whenever you add or retire a system, device or person.

Project | Typically needs an IT partner

Sources: 16 CFR 314.4, FTC Guide

SAMPLE

14 No secure disposal or retention process

MEDIUM

Secure disposal & retention · Your answer: Partially in place · §314.4(c)(6)

WHY IT MATTERS

Data you no longer need is pure risk. If it is not there, it cannot be stolen.

WHAT TO DO

- Write a retention schedule that reflects your legal retention obligations.
- Shred paper and securely wipe or destroy drives, copiers and printers before disposal.
- Review the retention policy at least yearly and purge data you no longer need.

Documentation | DIY-friendly

Sources: 16 CFR 314.4, FTC Guide, IRS Pub 4557

15 Safeguards not tested or monitored

MEDIUM

Safeguard testing & monitoring · Your answer: Partially in place · §314.4(d)(1)

WHY IT MATTERS

Controls drift: MFA gets switched off, backups fail quietly, encryption is never enabled on a new laptop. Regular checks catch it before an attacker does.

WHAT TO DO

- Set a regular schedule to confirm key controls are working: MFA, encryption, backups, updates and security alerts.
- Use monitoring that alerts on attacks or intrusions and make sure someone responds.
- Record each check and what was fixed.

Project | Typically needs an IT partner

Sources: 16 CFR 314.4, FTC Guide

16 No change-management procedure

MEDIUM

Change management · Your answer: Not in place · §314.4(c)(7)

WHY IT MATTERS

A rushed new app or router can quietly undo your protections. A short review before changes keeps security intact.

WHAT TO DO

- Require a short security review before adding or changing systems, software or network gear.
- Log changes: what changed, who approved it, and when.
- Update your inventory and risk assessment after significant changes.

Documentation | DIY-friendly

Sources: 16 CFR 314.4, FTC Guide

SAMPLE

17 Vendor oversight gaps

MEDIUM

Vendor oversight · Your answer: Partially in place · §314.4(f)

WHY IT MATTERS

Breaches at IT, software and payroll vendors often expose their clients. Contracts and periodic checks keep your firm protected and on record.

WHAT TO DO

- Identify every vendor with access to client data (IT, software, cloud, shredding, payroll).
- Add security requirements to contracts.
- Reassess higher-risk vendors at least yearly and keep the results on file.

Documentation DIY-friendly

Sources: 16 CFR 314.4, FTC Guide

18 Apps handling client data not evaluated

MEDIUM

App security review · Your answer: Partially in place · §314.4(c)(4)

WHY IT MATTERS

Your client data is only as safe as the weakest app that holds it. A quick check before you adopt a tool avoids surprises.

WHAT TO DO

- List every app that stores or transmits client data.
- Check each for MFA, encryption and the vendor's security attestations (for example SOC 2).
- Re-evaluate when you adopt new tools or the vendor changes significantly.

Documentation DIY-friendly

Sources: 16 CFR 314.4, FTC Guide

SAMPLE

05 · EVIDENCE BINDER

2 of 16 documents ready

The documents a regulator, cyber insurer or client is likely to ask for, derived from your answers. Ready = answered Yes; Incomplete = partly in place; Missing = No or Not sure.

STATUS	DOCUMENT	BASIS
INCOMPLETE	Written information security program (WISP)	§314.3(a) · Pub 5708
READY	Qualified Individual designation	§314.4(a)
MISSING	Written risk assessment	§314.4(b)(1)
INCOMPLETE	Data and asset inventory	§314.4(c)(2)
MISSING	Access review records	§314.4(c)(1)
INCOMPLETE	MFA coverage and written exception approvals	§314.4(c)(5)
INCOMPLETE	Encryption records and QI-approved compensating controls	§314.4(c)(3)
INCOMPLETE	Data retention and disposal policy	§314.4(c)(6)
MISSING	Change-management log	§314.4(c)(7)
INCOMPLETE	Activity logs and monitoring records	§314.4(c)(8) · (d)(1)
MISSING	Penetration test and vulnerability scan reports (or continuous-monitoring evidence)	§314.4(d)(2)
READY	Security training records	§314.4(e)
INCOMPLETE	Vendor contracts and oversight assessments	§314.4(f)
MISSING	Written incident response plan	§314.4(h) · Pub 5708
MISSING	FTC breach-notification procedure	§314.4(j)
MISSING	Annual written report to leadership	§314.4(i)

SAMPLE

06 · FULL ANSWER SUMMARY

Your answers

25 controls across 7 areas.

#	CONTROL	AREA	CITATION	ANSWER
1	Qualified Individual	Governance	§314.4(a)	Yes
2	Written security plan (WISP)	Governance	§314.3(a)	Partial
3	Annual report to leadership	Governance	§314.4(i)	No
4	Risk assessment	Risk	§314.4(b)	Partial
5	Written risk assessment	Risk	§314.4(b)(1)	No
6	Data & asset inventory	Risk	§314.4(c)(2)	Partial
7	Unique logins & least privilege	Access	§314.4(c)(1)	Yes
8	Periodic access reviews	Access	§314.4(c)(1)	No
9	Multi-factor authentication (MFA)	Access	§314.4(c)(5)	Partial
10	Encryption at rest	Data	§314.4(c)(3)	Yes
11	Encryption in transit	Data	§314.4(c)(3)	Not sure
12	Secure disposal & retention	Data	§314.4(c)(6)	Partial
13	Protected backups	Data	Pub 4557	Yes
14	Endpoint protection & updates	Systems	Pub 4557	Yes
15	Activity logging	Systems	§314.4(c)(8)	No
16	Safeguard testing & monitoring	Systems	§314.4(d)(1)	Partial
17	Pen testing & vulnerability scans	Systems	§314.4(d)(2)	No
18	Change management	Systems	§314.4(c)(7)	No
19	App security review	Systems	§314.4(c)(4)	Partial
20	Security awareness training	People	§314.4(e)	Yes
21	Vendor oversight	People	§314.4(f)	Partial
22	Incident response plan	Response	§314.4(h)	No
23	FTC breach notice procedure	Response	§314.4(j)	No
24	EFIN/PTIN monitoring	Response	Pub 4557	Yes
25	IRS data-theft reporting	Response	Pub 4557	Not sure

SAMPLE

07 · NEXT STEPS

Want these gaps closed before your next tax season?

ABT has run IT and cybersecurity for Boston-area businesses since 2003, including CPA and tax practices. We'll walk through this report with you and build a practical plan to close the gaps.

ABT handles every item on this list as a managed service.

Book a free consultation

Call (508) 586-1000

Sources

1. 16 CFR Part 314, Standards for Safeguarding Customer Information, §314.4 Elements.
   https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314/section-314.4
2. 16 CFR §314.3 Standards for safeguarding customer information (written information security program).
   https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314/section-314.3
3. 16 CFR §314.6 Exceptions (fewer than 5,000 consumers).
   https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314/section-314.6
4. FTC, "FTC Safeguards Rule: What Your Business Needs to Know".
   https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know
5. IRS Publication 4557, Safeguarding Taxpayer Data (Rev. 6-2024).
   https://www.irs.gov/pub/irs-pdf/p4557.pdf
6. IRS Publication 5708, Creating a Written Information Security Plan (WISP) for Your Tax & Accounting Practice (Rev. 8-2024).
   https://www.irs.gov/pub/irs-pdf/p5708.pdf
7. IRS Instructions for Form W-12, PTIN Application and Renewal (Rev. 10-2025), Line 11.
   https://www.irs.gov/pub/irs-pdf/iw12.pdf

Not legal advice. This report is generated from a self-assessment and is an educational tool based on public FTC and IRS guidance. It does not determine legal compliance and is not a substitute for advice from qualified legal, compliance or security professionals. Answers were provided by the firm and have not been independently verified. Scoring weights and risk bands were set by ABT and are not defined by the FTC or IRS.

Provided by All Business Technologies. Not affiliated with or endorsed by the FTC or IRS.