3rd element CONSULTING

FTC SAFEGUARDS RULE

Compliance Checklist

A practical, plain-language self-assessment for businesses covered by the FTC Safeguards Rule — updated for the current breach notification and exemption thresholds.

3rd Element Consulting · 2026 Edition

Before you check any boxes.

This checklist reflects the requirements of the FTC Safeguards Rule in plain language. Use it to find out where your business actually stands — not to guess.

Most businesses covered by the Safeguards Rule misunderstand one thing before they misunderstand anything else: what the size-based exemption actually covers. Getting this wrong is the most common reason a covered business has nothing in place at all.

Two numbers. Two different things.

5,000 records	What it means
The exemption threshold	A cumulative count of every consumer whose information your business has ever maintained — not your current client list. Businesses under this threshold are exempt from three specific requirements only: a written risk assessment, a documented incident response plan, and annual board reporting. Everything else in the rule still applies.
500 records	**What it means**
The breach notification threshold	If a security event involves unauthorized access to 500 or more consumers' unencrypted information, the rule requires notifying the FTC within 30 days of discovery — regardless of whether your business qualifies for the exemption above.

One more thing worth knowing: even if the Safeguards Rule doesn't require an incident response plan for your business, your cyber insurance carrier likely does. Most applications ask for one regardless of your size or regulatory exemption.

Who this applies to.

The rule applies to a broad category of "financial institutions" under FTC jurisdiction — including mortgage lenders, finance companies, account servicers, collection agencies, credit counselors and financial advisors, tax preparation firms, investment advisors not required to register with the SEC, and businesses that broker financial transactions. If your business prepares tax returns, advises on financial matters, services accounts, or extends credit, you are very likely covered.

The checklist.

Check each item only if it is actually true today — not if it is planned, partially done, or assumed. An honest "no" is more useful than an optimistic "yes."

GOVERNANCE & ACCOUNTABILITY

- [ ] I have designated a Qualified Individual to implement and supervise our information security program.

  This person does not need a specific degree or certification — but they need to be named, and the responsibility needs to be documented, even if an outside provider helps implement the program.

- [ ] I understand that hiring an IT provider does not transfer our legal responsibility for this program.

  The rule is explicit: someone inside the business still has to be accountable for overseeing the relationship.

- [ ] I have a written information security plan (WISP) that reflects what is actually in place — not a generic template that was never customized.

- [ ] I have conducted and documented a data and system inventory of all information our business collects, stores, and transmits.

RISK ASSESSMENT & PLANNING

- [ ] I have conducted a written risk assessment, including risk criteria and how our program addresses and mitigates them.

  Not required if your business is under the 5,000-record threshold — but still a sound practice regardless.

- [ ] I conduct additional periodic risk assessments, not just a single one-time assessment.

The checklist, continued.

RISK ASSESSMENT & PLANNING

- [ ] I have a written, documented incident response plan, including goals, a communications plan, and defined roles and responsibilities.

  Not required by the rule if you are under 5,000 records — but almost always required by your cyber insurance carrier regardless.

ACCESS & AUTHENTICATION

- [ ] I have implemented technical and physical access controls limiting who can reach customer information.
- [ ] I have multi-factor authentication (MFA) enabled and enforced for all systems containing sensitive customer information.

  Enabled and enforced are different things. Confirm it is required, not optional.

DATA PROTECTION

- [ ] I have ensured encryption of all customer information in transit and at rest.
- [ ] I have documented retention and disposal procedures for customer information.

MONITORING & CHANGE MANAGEMENT

- [ ] I have established change management procedures for modifying information systems.
- [ ] I have implemented policies, procedures, and controls to monitor and log activity.

The checklist, continued.

VENDOR & CONTINUOUS REVIEW

- [ ] I perform (or have a provider perform) regular penetration testing, vulnerability assessments, and vendor risk assessments.

REPORTING & REVIEW

- [ ] I provide regular reports on compliance and our overall cyber hygiene status to ownership or leadership.

  Annual board reporting is not required if you are under the 5,000-record threshold — but leadership should still see this regularly.

- [ ] If a breach occurs involving 500 or more consumer records, I know how to notify the FTC within 30 days of discovery.

  This requirement applies regardless of your size or exemption status.

If you checked “no” more than once.

That is normal, and it is exactly the gap an IT Environment Review is built to find. We look at what is actually in place, compare it against what the rule requires, and tell you where the gaps are — not a sales call, a real look at where things stand.

Schedule an IT Environment Review