# FTC Safeguards Quick Compliance Checklist

For CPA Firms and Tax Professionals

The FTC Safeguards Rule requires all CPA firms to implement a set of security controls to protect client financial data. Use this quick checklist to see where your firm stands. Mark Yes or No for each requirement.

## 1. Governance and Security Leadership

Yes: ☐ No: ☐ We have a designated qualified person responsible for our security program. We

Yes: ☐ No: ☐ review our security program at least once per year.

Yes: ☐ No: ☐ We have written policies for data handling, access control, and security expectations.

## 2. Risk Assessment

Yes: ☐ No: ☐ We have completed a formal risk assessment in the past 12 months.

Yes: ☐ No: ☐ Our assessment identifies both internal and external risks to client data. We have

Yes: ☐ No: ☐ documented mitigation steps for each identified risk.

## 3. Access Controls

Yes: ☐ No: ☐ All user accounts require strong, complex passwords.

Yes: ☐ No: ☐ Multifactor authentication (MFA) is enabled for all staff.

Yes: ☐ No: ☐ We limit access to client data to only essential personnel.

## 4. Encryption

Yes: ☐ No: ☐ Client data is encrypted at rest on all devices.

Yes: ☐ No: ☐ Client data is encrypted in transit.

## 5. Secure Data Storage and Disposal

Yes: ☐ No: ☐ We securely store all sensitive client records.

Yes: ☐ No: ☐ We have a formal retention and destruction policy.

Yes: ☐ No: ☐ We securely dispose of old files, devices, and backups.

## 6. Monitoring and Threat Detection

Yes: ☐ No: ☐ We use antivirus or EDR on all workstations and servers.

Yes: ☐ No: ☐ We actively monitor for suspicious activity.

Yes: ☐ No: ☐ We receive alerts when security issues occur.

# FTC Safeguards Quick Compliance Checklist (Continued)

### 7. Vendor Management

Yes: ☐ No: ☐ We maintain a list of all vendors who handle or store client data.

Yes: ☐ No: ☐ We verify the security of each vendor.

Yes: ☐ No: ☐ We have signed agreements defining security responsibilities.

### 8. Employee Security Training

Yes: ☐ No: ☐ All staff receive security awareness training at least once per year.

Yes: ☐ No: ☐ We conduct phishing simulations or similar tests.

Yes: ☐ No: ☐ We follow documented onboarding and offboarding procedures.

### 9. Incident Response

Yes: ☐ No: ☐ We have a documented incident response plan.

Yes: ☐ No: ☐ Staff know who to contact during an incident.

Yes: ☐ No: ☐ We retain logs needed for investigations.

### Your Score

Count the number of “No” responses:

0–3 No’s: Mostly compliant, but improvements recommended.
4–7 No’s: Significant risks exist. You are likely not compliant.
8+ No’s: High exposure to FTC penalties and insurance denial. Immediate action recommended.

### Need More Detail?

Download the expanded version for deeper explanations, examples, and remediation guidance.

■ Download the Expanded Guide

### Want a Professional Assessment?

Schedule a Safeguards Readiness Call:

■ Book Your Assessment