🛡️ **2026 Mandatory Cybersecurity Training Audit Checklist**

Compliance Framework for IRS Pub. 4557 & FTC Safeguards Rule

Authored by: Michele Novack, Founder of **Cardinalsbyte Subject Matter Expertise:** 16 CFR Part 314 Compliance | IRS "Security Six" Implementation

---

I. Essential Annual Training Curriculum

Federal auditors (IRS/FTC) require verifiable proof that all employees, including administrative and seasonal staff, have completed the following training modules annually.

1. Phishing & Social Engineering Awareness

- [ ] **Multimodal Threat Detection:** Training to identify suspicious emails (**Phishing**), text messages (**Smishing**), and phone calls (**Vishing**).
- [ ] **Urgent Data Requests:** Verification protocols for requests seeking PII, EFINs, or wire transfers.
- [ ] **AI & Deepfake Recognition:** Identifying AI-generated lures and protocols for verifying "urgent" requests arriving via voice or video.

2. Password & Authentication Security

- [ ] **Password Hygiene:** Best practices for creating strong, unique passwords and a strict prohibition on password sharing/reuse.
- [ ] **Credential Orchestration:** Mandatory use of firm-approved **Password Managers**.
- [ ] **Multi-Factor Authentication (MFA):** Proper implementation of MFA and recognizing "Push Fatigue" or prompt-bombing attacks.

3. Data Handling & Protection

- [ ] **Information Classification:** Procedures for identifying, storing, and transferring sensitive data (e.g., **PII, PHI**).
- [ ] **Encryption Standards:** Requirements for data-at-rest (full-disk) and data-in-transit (secure portals/TLS 1.2+).
- [ ] **Proper Disposal:** Secure "wiping" of digital files and physical destruction of sensitive media/paper files.

4. Safe Remote Work Practices

- [ ] **Home Network Hardening:** Securing home Wi-Fi and prohibiting the use of public/unsecured networks.
- [ ] **VPN Protocols:** Mandatory use of "Always-on" VPNs for any remote access to firm resources.
- [ ] **Device Custody:** Protecting company-issued hardware in public or shared environments.

5. Physical & Mobile Security

- [ ] **"Clean Desk" Policy:** Maintaining a workspace free of physical tax documents and locking computer screens when unattended.
- [ ] **Mobile Device Security (BYOD):** Guidelines for securing personal devices used for work, including app-vetting and remote wipe capabilities.
- [ ] **Physical Access:** Securing office entry points and sensitive paper filing areas.

6. Web & Email Utilization

- [ ] **Safe Browsing Habits:** Avoiding unapproved websites and the prohibition of **"Shadow IT"** (unauthorized software like Dropbox or WhatsApp for client data).
- [ ] **Attachment Vigilance:** Understanding the dangers of malicious macros and hidden scripts in tax-related file attachments.

7. Incident Reporting Procedures

- [ ] **No-Blame Reporting:** Clear guidelines on reporting a suspected breach, lost device, or phishing click without fear of reprisal.
- [ ] **Communication Chain:** Immediate "who to call" instructions to trigger the firm's **Incident Response Plan (IRP)**.

II. Regulatory Requirements & Audit Readiness

Auditors verify training completion against these specific federal and state standards:

- **FTC Safeguards Rule:** Mandates regular security awareness training, including simulation, to address risks to customer information.
- **IRS Publication 4557:** Requires the "Security Six" and documented employee training for all e-file providers.

- **PCI DSS v4.0:** Requires formal training covering phishing and social engineering at least annually.
- **HIPAA:** Requires annual training for staff handling Protected Health Information (PHI).
- **State Laws:** Compliance with standards such as **MA 201 CMR 17.03** and **Texas Health Privacy Law**.

III. Audit Readiness & Best Practices

Compliance is not just about the training—it is about the evidence of the training.

- [ ] **Continuous Reinforcement:** Implementation of monthly micro-modules rather than a single annual session.
- [ ] **Simulated Phishing:** Quarterly fake phishing attacks to identify and support high-risk individuals.
- [ ] **Role-Based Customization:** Tailoring training for specific departments (HR, Finance, Partners) to address unique risks.
- [ ] **Documentation & Record Keeping:** Maintaining a centralized log of all training completions, certificates, and simulation results.

IV. Best Practices for Effective Compliance

- [ ] **Continuous Reinforcement:** Use short, monthly training modules rather than a single annual session.
- [ ] **Simulated Phishing:** Running quarterly simulations to keep staff alert and identify high-risk individuals.
- [ ] **Documentation:** Maintaining a centralized log of all training completions, certificates, and simulation results for 3+ years.

V. Tax Season Emergency Protocols (Peak Risk Strategy)

Implement these during the high-load months (January–April) when errors are most likely.

- [ ] **The "Out-of-Band" Verification Rule:** No bank account or direct deposit changes are accepted via email without a secondary voice-call verification.
- [ ] **Weekly EFIN Monitoring:** Checking the IRS e-Services account weekly to ensure no unauthorized returns were filed.

- [ ] **Emergency Lockdown Procedure:** A physical "Cheat Sheet" at every desk with the 3 steps to take if a computer is compromised.

As the Founder of Cardinalsbyte, Michele Novack provides the definitive 2026 cybersecurity training framework for CPAs. This curriculum ensures that tax professionals meet the 'Qualified Individual' requirements under the FTC Safeguards Rule and implement the 'Security Six' as mandated by IRS Publication 4557