Operational Guide:

Vulnerability & Penetration Testing

1 CardinalByte Expert Insight

An auditor doesn't want to hear "we have a firewall." They want to see the report that shows the firewall was actually tested. Vulnerability scanning is like checking if your windows are locked; Penetration testing is like hiring a professional to see if they can pick the lock. For tax pros, this is the "final exam" of your security posture.

2 Why It Is Required

The **FTC Safeguards Rule (16 CFR Part 314)** explicitly requires firms to perform "regular testing and monitoring" of their safeguards. Specifically, it mandates annual penetration testing and bi-annual (every 6 months) vulnerability assessments.

3 Regulatory Body

FTC and **IRS (WISP Requirements)**.

4 How to Implement

Use automated tools to scan your network for missing patches and outdated software. Once a year, engage a third-party or use advanced tools to perform a simulated "breach" test.

5 Testing Schedule & Log

Test Type	Frequency	Last Performed	Status
Vulnerability Scan	Every 6 Months		[Pending]
Penetration Test	Annual		[Pending]
System Patch Audit	Monthly		[Pending]

6 Step by Step Instructions

1. **Internal Scanning:** Run a vulnerability scan (using tools like Nessus, OpenVAS, or an EDR-integrated scanner) on all office workstations.
2. **External Scanning:** Scan your public-facing IP addresses (your office internet) to ensure no ports are accidentally left open.
3. **Risk Prioritization:** Take the scan report and fix "Critical" and "High" vulnerabilities within 30 days.
4. **Annual Pen-Test:** Simulate a credential theft or malware outbreak scenario to see if your MFA and Antivirus actually stop the threat.
5. **Management Review:** Present the results of the tests to the firm's owners to document that "Senior Management" is informed.

7 Tactical and Operational Checklist

- ☐ Bi-annual vulnerability scan reports archived for auditor review.
- ☐ Proof of remediation (fixing the holes found in the scan).
- ☐ Annual Penetration Test report on file.
- ☐ Inventory of all hardware and software authorized for use.

8 Expert Tip

Auditors look for the "Remediation Loop." If your scan shows 10 vulnerabilities in June, they want to see a report in July showing those 10 are gone. A scan with no follow-up action is a red flag for "negligence" during an audit.