

FTC Safeguards Checklist For Financial Institutions

FTC Safeguard Rules are going into effect on **December 9, 2022.**
Have you checked off all the boxes?

Part 1: Required Policies

Designated Qualified Individual

An individual on the IT/security team who oversees the security program. They must have skills that are considered “adequate” for the amount of data you're processing and/or storing.

Options:

- Current employee with the qualifications/training or hire someone new.
- If you can't support a full-time resource, leverage a *fractional* resource (vCISO) from a service provider.

Note: Ultimately, the organization retains responsibility.

Incident Response Plan

This plan details a series of actions that the security team must take in the event of a cyber incident: Preparation; Detection & Analysis; Containment, Eradication & Recovery; and Post-Incident Activities.

Options:

- Develop an incident response plan internally.
- Collaborate with a managed service provider.

Tips:



Perform “Tabletop Exercises” to validate your organization’s readiness, identify areas for improvement, and train new staff.

Information Access Controls, Disposal Plan & Change Management

Information access controls restrict who can make changes and creates an audit trail of all changes.

Change management details what process you should follow when your technology stack changes.

A **disposal plan** lays out the process for secure disposal of customer information. The Safeguards Rule requires a limit of two years — with some exceptions.

Options:

- Work with a managed service provider to Hire an outsourced firm to help create them
- Develop these policies internally with help from free templates

Oversee Service Providers & Apps

Review your applications and vendors that you share data with. If they are also handling financial data, they too must comply with all of these safeguards. And, unfortunately you're on the hook if they're not.

Options:

- Research and select vendors that already meet these safeguards

Tips:



Share this checklist with your vendors and keep it handy for future vendor discussions. Make sure they're aware these safeguards apply to them. Look for vendors with certifications, such as SOC 2 Type 2.

Does This Affect Me?

- Auto dealerships
- Mortgage lenders or brokers
- Tax preparation firms
- Payday lenders
- Finance companies
- Check cashers/wire transferors
- Collection agencies
- Credit counselors
- Financial advisors

Part 2: Reports and Documentation

Data and Systems Inventory

Just like you have to track the cars on your lots, the FTC requires you have an inventory of all data you have stored and the systems they're on.

Options:

- Create your own documentation using a simple Excel spreadsheet
- Find a software solution such as Oracle NetSuite Look for a consulting service

Tips:



A common challenge with inventory is keeping it up-to-date. You can't protect what you don't have. Leverage automation and tools such as Nmap; it provides a plethora of information about your network.

Risk Assessment

This involves identifying threats to an environment — both internal and external — to the security, confidentiality, and integrity of customer information. This written assessment must include criteria for evaluating those risks and threats.

Options:

- Perform a self-assessment to prepare for a 3rd party assessment
- Outsource to a qualified managed service provider

Tips:



Use a framework such as NIST Cyber Security Framework (CSF) to benchmark your organization and identify gaps for remediation.

Information Security Program

Really, this whole checklist is your information security program. Developing one is an ongoing process that requires an understanding of the different facets of security described here, and more.

Options:

- Create it in-house
- Collaborate with a qualified managed service provider

Tips:



When building a security program, it's best to work with experts who have experience creating them before. Work with a service provider who already safeguards their own data and has helped numerous customers with their security program. Remember: People, Process, Technology, you need all 3 to make a security program successful.

Report To Your Board of Directors

Your Qualified Individual must give an update to your Board of Directors (or a Senior Officer if there isn't a board) on a regular basis — at least once a year.

Tips:



Match your existing reporting by pulling reports and key insights from the security tools you've already implemented. Set up the reports on a standard recurring basis so everyone knows exactly when they are.

Part 3: Technical Requirements

Multi-factor Authentication

Enable multi-factor authentication on all systems that employees and contractors log into. MFA is an easy way to add another layer of verification of a user's identity and prevent the success of attacks like phishing, stolen credentials and account takeovers.

Options:

- Ask your service provider to implement
- MFA vendors such as Duo Security, Okta, Microsoft

Tips:



Take advantage of built-in features from tools that you already use. For example, if you already run Microsoft 365, take advantage of the ability to enable MFA for free across your environment.

Data Encryption

Encrypt customer information on your system and when it's in transit. If it's not feasible to use encryption, secure it by using effective alternative controls approved by the Qualified Individual who supervises your information security program.

Options:

- Use encryption vendors such as BitLocker, FireVault
- Built-in tools

Penetration Testing and Vulnerability Assessments

Penetration testing, vulnerability assessments and continuous monitoring all help to detect both actual and attempted attacks. Continuous monitoring is an excellent way to test your environment.

Without **continuous monitoring**, you must conduct annual **penetration testing** and **vulnerability assessments**, including system-wide scans every six months to test publicly-known vulnerabilities.

Options:

- Implement an in-house vulnerability management program using tools such as Tenable or Qualys, or outsource to a managed service provider
- Hire a qualified pen testing firm to find the weak points in your security – *and remediate them*

Tips:



While both are valuable, understand the difference between a vulnerability scan and a penetration test. A penetration test goes the extra step to exploit the vulnerabilities

Monitor and Log Authorized and Suspicious Activity

Implement a Security Information & Event Management (SIEM) solution to monitor when authorized users are accessing customer information on your system and to detect unauthorized or suspicious access.

Options:

- Build out an internal Security Operations Center (SOC) – hire a team of trained security analysts to monitor, investigate, and respond to the SIEM alerts.
- Outsource to a qualified managed security service provider.

Tips:



Common challenges of building out your own SOC and managing a SIEM in-house include a major skills shortage, 24x7 coverage, and alert fatigue. Partnering with managed security service provider (MSSP) may alleviate these issues.

Part 4: Training Requirements

Employee Security Awareness Training

Provide your people with security awareness training and schedule regular refreshers.

Options:

- Implement a security awareness program
- Outsource to a qualified managed security provider

Tips:



Security Awareness Training needs to be on-going, not just a single video annually. Use simulated phishing campaigns to test your users' knowledge and provide additional training as needed.

Training and Security Updates for Security Personnel

Provide specialized training for employees, affiliates, or service providers who are hands-on with your information security program and verify that they're monitoring the latest word on emerging threats and countermeasures.

Options:

- Online certification courses




Tips:



This is a great opportunity to promote growth on your team. Helping individuals in leveling up their career is a great way to show support.

Why Appalachia?

Meet compliance controls, save time on security tasks, focus on real threats and protect against a breach faster than ever with Appalachia Technologies.

 <p>AUTOMATE TASKS FOR YOU</p> <p>We do all the heavy lifting for your team to save them time, including parsing, creating native third-party integrations, and testing and tuning detection rules to reduce noisy alerts.</p>	 <p>FASTER TIME TO SECURITY</p> <p>Our unique approach to detections notifies you of threats other security tools may miss, sending you real-time alerts in under a minute of initial detection to help you respond to threats faster than ever.</p>	 <p>EASILY MEET COMPLIANCE</p> <p>With a year of data retention and deployment that takes minutes to hours, we help you meet cyber insurance and compliance easily and quickly with the team you have today.</p>
--	--	--

Contact us at info@appalachiatech.com to learn how we can help **YOUR** organization check **ALL** of the boxes!

