ABSOLUTE
PERFORMANCE

While every company is different, the FTC has set a minimum standard for how you should protect your customer's data. Use the questions below to do a quick gut check to see how you would line up with the Safeguards Rule.

1. ____________________ is responsible for our Security Program. They have __ years of experience and _____________ Certifications. They report to the board every _____________.

2. Our most recent Risk Assessment was completed on ________. Our biggest risk was ___________________ and we ___________ to mitigate it.

3. We conducted our last Network Penetration Test on __ and confirmed everything was fixed on ________.

4. We train our employees to recognize phishing and other social engineering attacks by ______________________, which we last did on _____.

5. Our contracts with vendors require them to __________________ to protect our data and customers, and we are contractually allowed to _________________ to confirm they are meeting our requirements.

6. We last reviewed our Security Program and Policies on ___________________.

7. In the event we were breached, we would ______________________________.

8. We review who has access to sensitive customer data, which we last did on __________.

9. We track where data is stored, processed or transmitted, which we last confirmed on ___________.

10. We protect customer data we store by encrypting it with an algorithm based on _______________.

11. Only allow users to access customer data if they authenticate using ___________, which provides Multi-factor authentication.

12. Regularly test our applications to make sure they don't have security vulnerabilities, like those in the OWASP Top 10, and the last test we did was on ___________.

13. Don't keep customer data longer than ___________ and regularly check to make sure we aren't keeping data longer than that by _______________.

14. As we make changes to our environment, we manage those changes, and make sure those changes don't impact our security, by _______________________.

15. We use ________________ to log system and user activity so we can detect and stop unauthorized access, and have it deployed across ______ % of our environment.

16. At the end of the day, I feel ___________________________________ about our ability to meet the FTC Safeguards and protect our customer's data.

Answers and guidance are on page 2.

Answer Key

1. A single individual should be the "Qualified Individual" and able to report to the board. This can be an external party, but needs to have sufficient Security experience or credentials (such as a CISSP, CISA, etc)
2. Risk assessments must be completed annually, and programs designed to mitigate risks identified
3. Pen Tests must be done annually, with vulnerability scans every 6 months
4. Security Awareness Training must be done annually. Phishing testing highly recommended.
5. Vendor contracts must include language such as "right to audit" that allow for companies to verify compliance. Compliance with industry standards, such as a SOC2, PCI, or NIST are also acceptable
6. Policies must be reviewed annually
7. Organizations must have a documented Incident Response Plan to guide the response to a breach. This must include goals, roles and responsibilities, Communication Plans, Remediation activities, and post mortem analysis. Generally, aligning to NIST standards will meet these requirements.
8. Privileged access reviews on a periodic basis, usually every 6 months, to confirm that only people with a legitimate business reason to access data can do so.
9. Maintain system and data inventories, and it is highly recommended to have data flow diagrams or data flow mappings, to show where data moves in the environment.
10. Data should be encrypted when it is stored at rest, usually with at least AES 128 encryption.
11. Multi-Factor authentication, such as Okta or Duo, must be used when accessing sensitive data or systems.
12. Web app tests should be conducted at least annually, often in conjunction with Pen Tests
13. Not keep customer data longer than 2 years after it was last accessed
14. Have a system in place to track, review, and approve changes to make sure they do not reduce the security of the environment.
15. Have a system to track access to systems and movement across the environment, usually with at least 70% of systems covered, including all domain controllers, data repositories, and other sensitive assets.

How to read your results:

- **13 or more** of your answers were in line with the answer key, Congratulations! You're probably close to, or already, complying with the FTC Safeguards!
- **8 to 12** of your answers were in line with the answer key, you have a bit of work to do, but can probably achieve compliance by focusing on a few large items
- **Less than 8** of your answers align with the answer key, you may want to do a more comprehensive review of your environment and security program to identify systematic initiatives that can provide quick wins to improve your security and build a long term plan for compliance

Regardless of how you scored, our team would be happy to help review your results and discuss your next steps on the path to FTC Safeguard Compliance.

Reach out to Jeramie Brookins at 720.272.4973
or jrb@absolute-performance.com to schedule your free consult.

Absolute-Performance.com
12303 Airport Way 100, Broomfield, CO 80021