

Secure & Defend: FTC Safeguards Compliance

Protecting nonpublic personal financial information under the Gramm-Leach-Bliley Act (GLBA).

The Mandate: If your business handles customer financial data, the FTC Safeguards Rule requires a comprehensive, documented cybersecurity program. Staying compliant is a regulatory requirement designed to prevent breaches and uphold customer trust.



The Anatomy of the Rule.

What is actually required:



Qualified Individual: Designate a specific leader to supervise the program.



Risk Assessments: Conduct periodic assessments and continuous reviews.



Implement Safeguards: Deploy access controls, encryption, and secure authentication.



Staff Training: Regularly test staff effectiveness and security awareness.



Vendor Oversight: Monitor service providers and require security commitments.



Incident Response: Maintain a written plan and comply with breach reporting.

The Price of Non-Compliance.

The cost of inaction:

Regulatory Penalties

Fines for failing to protect data under GLBA.

Legal Action

Civil lawsuits and damages from affected customers.

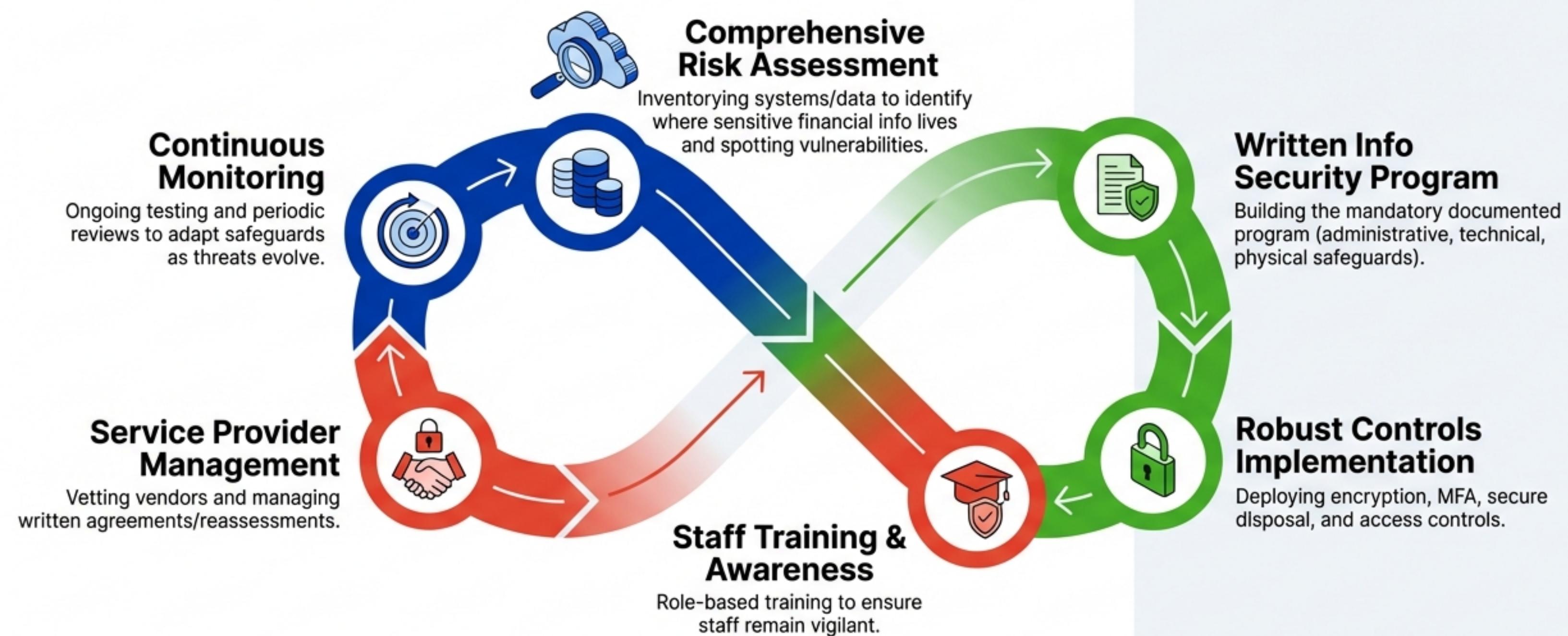
Reputation

Erosion of trust and loss of competitive advantage.

Operational Risk

Exposure to evolving cyber threats without defense.

From Assessment to Maintenance: How We Achieve Compliance



Why Partner With Us?

Regulatory & Security Experts

We understand both the technical implementation and the regulatory nuance of the Safeguards Rule.

Customized Roadmaps

Solutions tailored specifically to your business size, structure, and risk tolerance.

Clear Communication

We demystify requirements and provide straightforward, action-oriented recommendations.

Don't leave your reputation unprotected. Partner with professionals who make compliance achievable.

[Contact a Safeguards Compliance Consultant](#)

