

FFIEC & GLBA SAFEGUARDS RULE.

GLBA's Safeguards Rule sets the federal legal requirement to protect customer financial data; FFIEC's examination handbook is how bank regulators actually check whether that requirement is being met. **A policy document that was never operationalized satisfies neither.**

- WRITTEN SECURITY PROGRAM
- QUALIFIED INDIVIDUAL
- ENCRYPTION & MFA
- BOARD REPORTING

01 THE MECHANISM



Two Frameworks, One Obligation
GLBA's Safeguards Rule is the federal law requiring a written information security program; **FFIEC's IT Examination Handbook is the supervisory framework** bank examiners use to assess whether institutions actually meet it.



The Written Information Security Program
Both converge on the same deliverable: a formal, governing-body-approved program covering risk assessment, access controls, encryption, and incident response — **not informal practices.**



Qualified Individual & Board Reporting
The 2021 Safeguards Rule amendment requires **a single named individual accountable for the program**, who reports to the board or governing body on its status and material risks.

02 THE FLOW

The Documented, Tested Program CONTAINED

1

A qualified individual owns a written risk assessment that's periodically reviewed and drives **concrete controls** — access restrictions, encryption, MFA — not a generic policy binder.

2

The program is tested on a defined cadence — continuous monitoring, or annual penetration testing plus biannual scans — with **findings tracked to remediation.**

3

The qualified individual reports program status and material incidents to the board regularly, so **governance has real visibility** into the institution's risk posture.

The Policy-on-Paper Program EXPOSED

1

A written information security policy exists but was **never operationalized** into actual controls — no enforced encryption, no MFA requirement, no real access restrictions.

2

Testing, if it happens at all, isn't documented or tracked to remediation, so **known gaps persist across exam cycles** without anyone owning the fix.

3

An examiner or the FTC discovers the gap between the policy document and actual practice, and a **routine finding becomes a formal enforcement action.**

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Risk Assessment & Qualified Individual	A written, periodically reviewed risk assessment owned by a single named individual accountable for the security program.
Technical Safeguards	Access controls, encryption of customer information at rest and in transit, and multi-factor authentication for anyone accessing it.
Testing & Monitoring	Continuous monitoring, or annual penetration testing plus biannual vulnerability scanning, with findings tracked through to remediation.
Incident Response & Governance Reporting	A written incident response plan and regular reporting from the qualified individual to the board or governing body.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
A Written Policy With No Operational Controls	No	A policy document never implemented into access restrictions, encryption, or MFA doesn't protect customer information or satisfy the Rule.
Believing GLBA Only Applies to Traditional Banks	No	The "financial institution" definition covers any business significantly engaged in financial activities, not just chartered banks.
Annual Risk Assessment With No Ongoing Testing	No	The Safeguards Rule requires continuous monitoring or a defined testing cadence — a once-a-year paper exercise misses drift.
No Named Accountable Individual	No	Without a designated qualified individual, no one is formally accountable for the program's effectiveness or board reporting.
Qualified Individual + Written Risk Assessment + Technical Controls + Regular Testing + Board Reporting	Yes	Matches what both GLBA's Safeguards Rule and FFIEC examiners actually expect to see documented and operational.

FFIEC & GLBA SAFEGUARDS RULE. ASSESS · SAFEGUARD · REPORT

05 PROGRAM OPERATIONS

GLBA's "financial institution" definition is broader than most people assume — it covers any business significantly engaged in financial activities, not just chartered banks and credit unions.

The Safeguards Rule's 2021 amendment made several previously optional practices mandatory. Encryption, MFA, and a named qualified individual are no longer best practices — they're requirements.

FFIEC and FTC oversight differ in enforcement mechanism. Bank examiners issue supervisory findings for depository institutions; the FTC pursues consent orders and civil penalties for others.

FFIEC retired its standalone Cybersecurity Assessment Tool in 2023, directing institutions toward frameworks like the NIST CSF instead — a program still built solely around the old CAT is dated.

06 CONTROL MAPPING

GLBA SAFEGUARDS RULE

Federal requirement for a written, comprehensive information security program protecting customer nonpublic personal information, enforced by the FTC for non-bank institutions.

FFIEC IT EXAM HANDBOOK

The supervisory framework federal and state bank examiners use to assess depository institutions' information security, business continuity, and IT operations.

NIST CYBERSECURITY FRAMEWORK

The framework FFIEC now points institutions toward following the 2023 retirement of its standalone Cybersecurity Assessment Tool.

GLBA PRETEXTING PROVISIONS

Prohibits obtaining customer financial information under false pretenses, addressing social-engineering attacks aimed at the institution directly.

07 WHAT THIS DOES NOT SOLVE

Non-Financial Data Protection

The Safeguards Rule protects customer nonpublic personal information specifically; it **doesn't govern health or employee records** outside that scope.

Fraud at the Transaction Layer

A compliant program protects systems and data; it **doesn't by itself stop wire fraud or account takeover** happening through otherwise-legitimate access.

Third-Party Risk Beyond the Contract

The Rule requires overseeing service providers by contract, but a **provider's own internal security failure** can still expose customer data despite a compliant contract.

Consumer Behavior

Strong institutional controls **don't protect a customer who is phished or socially engineered** outside the institution's own systems.

08 MYTHS VS. REALITY

MYTH "GLBA only applies to banks and credit unions."	REALITY The "financial institution" definition covers any business significantly engaged in financial activities, including mortgage lenders and auto dealers arranging financing.
MYTH "Having a written security policy satisfies the Safeguards Rule."	REALITY The 2021 amendment requires specific operational controls — encryption, MFA, access restrictions, regular testing — not just a policy document.
MYTH "FFIEC guidance and the GLBA Safeguards Rule are the same requirement."	REALITY GLBA's Safeguards Rule is federal law; FFIEC's handbook is the supervisory framework examiners use — enforced through different mechanisms for different institution types.
MYTH "Encryption is mandatory under the Rule with no exceptions."	REALITY The Rule allows compensating controls when encryption is infeasible, but that determination must be reviewed and documented, not simply assumed.
MYTH "The FFIEC Cybersecurity Assessment Tool is still the standard reference."	REALITY FFIEC retired the standalone CAT in 2023 and now points institutions toward frameworks like the NIST CSF.

09 SPEAK THE PROGRAM — KEY TERMS

WISP (WRITTEN INFORMATION SECURITY PROGRAM)

The formal, governing-body-approved security program both GLBA and FFIEC expectations converge on, **covering risk assessment through incident response**.

QUALIFIED INDIVIDUAL

The single named person the 2021 Safeguards Rule amendment requires to be **accountable for the security program** and to report to the board.

NONPUBLIC PERSONAL INFORMATION (NPI)

The category of customer financial information GLBA's Safeguards Rule **specifically requires financial institutions to protect**.

FFIEC IT EXAMINATION HANDBOOK

The series of booklets federal and state examiners use to **assess a depository institution's information security** and IT risk management.

MATTERS REQUIRING ATTENTION (MRA)

A formal examiner finding requiring a depository institution to **remediate an identified deficiency**, short of a formal enforcement action.

FINANCIAL INSTITUTION (GLBA DEFINITION)

A broad category covering any business **significantly engaged in financial activities**, not limited to traditional chartered banks.