# The Three Lines of Defense for Cybersecurity Compliance

## Best practices for risk management and audit assurance

By Anna DeSimone

The foundation of modern financial privacy in America began in the year 1999 with the enactment of the Gramm-Leach-Bliley Act (GLBA). Over the next 10 years, the financial services industry saw the introduction of more regulations aimed at protecting confidential consumer information. The GLBA Safeguards Rule (16 CFR Part 314), enforced by the Federal Trade Commission (FTC), requires financial institutions to protect the security, confidentiality and integrity of customer information.

Companies subject to FTC jurisdiction include mortgage brokers, mortgage lenders, collection agencies, credit counselors, financial advisers, tax preparation firms, payday lenders and other entities engaged in activities that are financial in nature or incidental to financial activities. The FTC updated the Safeguards Rule in 2024, requiring all covered entities to establish a written information security program and a documented security risk program. The amended rule also requires entities to report certain data breaches and security incidents to the FTC.

The era of comprehensive state privacy laws began in 2020 with the California Privacy Rights Act, followed by the rapid spread of state legislation. Every U.S. state now requires mortgage lenders to maintain an information security program. While GLBA applies nationwide, most states have duplicated or expanded upon federal laws for licensees regulated by their Department of Financial Institutions, Department of Banking or similar agency.

States with explicit requirements as a condition of licensing or ongoing compliance include California, Connecticut, Illinois, Maryland, Massachusetts, Nevada, New York, Texas and Vermont. States requiring reference to GLBA and the FTC Safeguard Rule in the Nationwide Multistate Licensing System (NMLS) include Florida, Georgia, North Carolina, Ohio and Washington.

**Anna DeSimone** is president of Housing Research LLC and provides consulting services and policy development in the areas of fair lending, loan operations, quality control, servicing and information security. She has written over 40 industry handbooks published by AllRegs, the MBA of America and the Federal Reserve Bank of Boston. www.housingresearchpress.com

### The Three Lines of Defense Risk Management Model

- **First Line:** Operational teams implement access controls, security settings and protocols for internal and vendor systems
- **Second Line:** Policy and compliance teams set standards, monitor controls and report cybersecurity risks to leadership
- **Third Line:** Independent auditors assess overall risk framework effectiveness and certify compliance with industry standards

Failure to maintain a plan can result in enforcement actions or license suspension. Companies have been fined for lacking written information security plans, encryption policies or incident response procedures. Penalties vary by state but typically include civil fines between $25,000 and $250,000 per violation. Enforcement actions can include cease-and-desist consent orders requiring immediate corrective actions, required adoption and submission of a compliant information security plan or mandated third-party audits for 12 to 24 months.

The Conference of State Bank Supervisors (CSBS) and state regulators work together to create consistent regulatory standards for nonbank firms through the adoption of model laws. CSBS's model laws provide a clear nationwide framework for state legislatures to enact and state regulatory agencies to implement.

The Nonbank Model Data Security Law is largely based on the FTC Safeguards Rule. It requires companies to develop, implement and maintain a comprehensive, written information security program that contains administrative, technical and physical safeguards that are appropriate to the company's size and complexity, as well as the nature and scope of its activities.

Government-sponsored enterprises Fannie Mae and Freddie Mac announced information security requirements that went into effect in September 2025. Fannie's requirements are published in its Information Security and Business Resiliency Supplement, requiring lenders, servicers and third-party originators (TPOs) to maintain robust information security and data protection programs. Freddie's requirements for information security and business continuity planning are published in sections 1301 and 1302 of its seller/servicer guide.

Service providers must have substantially similar information security. Mandates published by both Fannie and Freddie include a provision whereby service providers who store, process, access or transmit confidential borrower information must comply with similar security and business continuity requirements. Known as "supply chain risk management," companies are expected to develop, document and implement formal vendor risk management controls to ensure the controls for new and existing vendors align with — and are as protective as — the company's information security program.

The widely used model for implementing an information security program is known as the "three lines of defense risk management model." The first line of defense applies to the people involved in daily operations and those responsible for making sure the information security program is running smoothly. First-line teams implement access controls, security settings and protocols for internal operations, as well as third-party and fourth-party service providers.

Second line of defense teams are tasked with establishing policy, standards and procedures. They provide expertise and guidance and monitor how well the first-line controls work. Second-line teams track compliance, perform risk assessment and report cybersecurity risks to leadership.

"Mandates published by both Fannie and Freddie include a provision whereby service providers who store, process, access or transmit confidential borrower information must comply with similar security and business continuity requirements."

The third line of defense provides objective and independent assurance. Internal or external auditors evaluate the effectiveness of the entire risk management framework, including controls managed by the first two lines. Auditor reports generally include attestations certifying compliance to industry standards such as the National Institute of Standards in Technology (NIST) framework, the International Organization for Standardization (ISO 27001) or Service Organization Controls 2 (SOC 2). ●