

A FOUR STEP ROADMAP TO COMPLYING WITH THE GLBA SAFEGUARD RULE

A Whitepaper By



Luciana Obregon

Security Architect

PayPal



Introduction

Financial institutions in the United States are governed by several government-established regulatory bodies designed to oversee the performance, transparency, and fairness of financial markets and their practices while protecting the interest of consumers, ensuring the confidentiality and privacy of personally identifiable information (PII), and preventing and investigating financial fraud. Amongst these regulatory bodies is the Federal Trade Commission (FTC), established on September 26, 1914, after President Woodrow Wilson enacted the Federal Trade Commission Act. The FTC's mission is to "*protect consumers and competition*" and has enforcement responsibilities under several consumer protection and antitrust laws, including Title V of the Gramm-Leach-Bliley Act, entitled "Disclosure of Nonpublic Personal Information".

The Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, was signed into law on November 12, 1999, by President Bill Clinton, and it was designed to reform the banking industry by allowing banking institutions to offer a wide range of services to consumers, such as insurance and securities brokerage. Regarding information security, the Act mandated financial institutions implement safeguards to protect the privacy and security of non-public personal information (NPPI) about consumers. Further to that, section 504 of the Act required the FTC, along with other banking agencies and regulatory bodies, to prescribe regulations necessary for financial institutions to meet the requirements set forth by the law.

The FTC, therefore, issued the [GLBA Privacy Rule](#) in 2000 to implement the privacy requirements outlined in *Title V, subtitle A* of the Act concerning sharing NPPI about consumers to nonaffiliated third parties, disclosing to customers the financial institutions' privacy policies and practices regarding information sharing with affiliated and non-affiliated third parties, and allowing customers to opt-out of having their information shared. Furthermore, the FTC enacted the [GLBA Safeguards Rule](#) in 2002 to establish standards to help financial institutions address the requirements outlined in Title V, subtitle B of the Act for financial institutions concerning the protection of NPPI about consumers through the implementation of comprehensive, risk-driven information security programs.

In 2019, the FTC proposed amending the GLBA Safeguards Rule with more specific and prescriptive security requirements for financial institutions to include in their information security program implementation. The proposed changes to the GLBA Safeguards Rule were based on New York's Cybersecurity Regulations implemented in 2017 and addressed requirements for people, process, and technology elements that underpin any information security program. At the time of this writing, the FTC has not published an amended version of the GLBA Safeguards Rule, therefore, this paper is based on the GLBA Safeguards Rule that became effective in 2003.

This whitepaper focuses exclusively on the GLBA Safeguards Rule and examines the information security requirements for financial institutions under the FTC's jurisdiction. Furthermore, the paper outlines a four-step roadmap for financial institutions to become compliant with the Act.

The GLBA Safeguards Rule

The FTC published the GLBA Safeguards Rule on May 23, 2002, in response to the requirements outlined in section 504, subtitle A, title V of the Gramm-Leach-Bliley Act, which required the FTC and other federal agencies to establish standards to protect certain types of information through the implementation of administrative, technical, and physical controls. The Rule took effect on May 23, 2003, requiring financial institutions to implement a comprehensive information security program designed to protect the security, confidentiality, and integrity of NPPI about consumers. As with any information security regulation and compliance standard, understanding its applicability to your business and your scope of compliance is essential to controlling the costs associated with information security activities and remediations.

Scope and Applicability

The scope of the Rule covers the handling (processing, storing, transmitting) of non-public consumers' personal information by any financial institution under the FTC's jurisdiction. Furthermore, the Rule defines non-public consumers' personal information as *"personally identifiable financial information"* that is not publicly available and that is:

1. Obtained by a financial institution directly from a consumer or indirectly from other financial institutions, or
2. Provided by a consumer to a financial institution, or
3. Collected by the financial institution from a consumer as a result of a transaction or service provided to the consumer

The Rule applies to financial institutions that handle NPPI, or any institution that engages in financial activities, as described in the Bank Holding Company Act of 1956, for instance, banks, car dealerships that offer loans, universities that offer student aid, payday lenders, check cashing institutions, to name a few.

While initially all financial institutions, regardless of size, were required to comply with the Rule, the 2019 proposed rule changes would exempt financial institutions with less than five thousand (5,000) costumers from most of the written requirements set forth by the Rule. Such financial institutions must still, however, comply with the basic security requirements outlined in the Rule.

Information Security Requirements under the GLBA Safeguards Rule

The standards outlined in the first publication of the GLBA Safeguards Rule include broad and non-prescriptive security requirements that financial institutions have to meet to become compliant with the law. The standards were written in this manner to give financial institutions enough flexibility to tailor the security requirements to the needs of their business while ensuring that the Rule's objectives are met.



The standards require financial institutions to develop, implement, and maintain a **written, comprehensive, and risk-driven information security program** that is appropriate to the size of the institution and includes the implementation of administrative, technical, and physical controls to protect the security, confidentiality, and integrity of NPPI about consumers. Thus, financial institutions are required to:

1. Appoint an **employee or group of employees** responsible for managing the information security program and accountable for ensuring that the program meets its defined objectives.
2. Establish an **information risk management capability** designed to identify, assess, rate, treat, communicate, and track *reasonably foreseeable internal and external risks* that could impact the security, confidentiality, or integrity of NPPI about consumers, minimally covering the following areas:
 - a. Employee training and management
 - b. Information systems, software, networks, and information processing, storage, transmission, and disposal
 - c. Security incident detection, prevention, and response and other system failures
3. **Design and implement technical, physical, and administrative controls** to manage identified risks and **regularly test or monitor their effectiveness**.
4. Establish an **external supplier risk management capability** designed to identify supply chain risks and ensure that external suppliers or service providers with which financial institutions engage are contractually bound to implement and maintain reasonable and suitable safeguards to protect NPPI about consumers in their custody.
5. **Evaluate and adjust the information security program** as a result of testing or when material changes to the business, cyber-threat landscape, or other circumstances impact the effectiveness of existing technical, administrative, or physical safeguards.

Safeguarding Non-Public Personal Information

By definition, security is “the state of being free from danger or threat” and has been used throughout history to protect people, property, or valuable information from known threats. Similarly, organizations use physical security to protect their employees and business property, and information security to protect information from physical and cyber threats. Generally, everything about a business can be somewhat represented by information, for instance how the business operates, its strategies, and successes and failures. Furthermore, organizations across all industry sectors depend on information technology and systems to carry out their mission and business objective, and those systems need also be protected against a wide range of threats. Additionally, business information can be broadly grouped into two categories:

- **Intellectual property**, or intangible assets that are created, owned, and legally protected by the organization against unauthorized use or disclosure. An example of intellectual property could be an organization's mergers and acquisitions strategy.

- **Protected or regulated information**, or information protected at the federal or state level under information protection or privacy laws, such as GLBA, GDPR, or HIPAA. An example of protected or regulated information is personally identifiable information or personal health information.

While organizations are responsible for establishing the requirements for protecting the confidentiality, integrity, and availability of their intellectual property and information systems, federal and state government bodies are generally responsible for establishing the requirements for protecting the privacy, security, and confidentiality of protected or regulated information and for obtaining assurance that those requirements are being met. Financial institutions are therefore accountable for implementing the requirements mandated by government bodies to protect regulated information in their custody.

Four Steps to Comply with the GLBA Safeguards Rule

In the next few sections, we will outline a roadmap to help financial institutions comply with the requirements set forth by the GLBA Safeguards Rule.

Step 1: Establish an Information Risk Management Capability

The GLBA Safeguards Rule requires financial institutions to develop a written information security program that is driven by “reasonably foreseeable internal and external risks”, but what does this mean? In essence, it means that different types of business information have different monetary values and will therefore be exposed to different types of information risks. Further to that, it means that information should be protected at levels that are commensurate with its risk profiles rather than uniformly because it is unrealistic to expect organizations to protect all of their information and systems with the same rigor. But how do we know what business information we need to protect and at what levels? With regards to regulations such as GLBA, it may seem natural to think that all NPPI must be protected at the same level. But NPPI is a broad category that covers various types of information elements, is processed by many different information systems, and is handled by various types of individuals. Applying the same level of protection to all NPPI notwithstanding the inherent risks resulting from the loss of privacy, confidentiality, or integrity of each information element could become very expensive for an organization. Hence the GLBA Safeguards Rule guidance of adopting a risk-based approach to protecting regulated information.

Understanding Information Risk Management

Information risk is the loss that an organization could endure if the confidentiality, integrity, and/or availability attributes of their information were compromised, and is often expressed as the product of two factors, including:

- o **Likelihood** or probability that a threat will exploit a vulnerability on an information system, and
- o **Impact** or ramifications to the organization resulting from the successful exploitation of a vulnerability



Or $\text{Risk} = \text{Likelihood} \times \text{Impact}$

Information risk management is the act of weighing information risk against reward and making business decisions based on the results of risk assessments. There are various industry-accepted risk assessment methodologies that you can adopt, such as NIST SP 800-30, ISO/IEC 27005, ISF IRAM2, and most of these methodologies follow a lifecycle approach to managing information risks. You should consider all methodologies and select one that meets the long-term needs of your organization.

Before you begin developing your information security program, you should conduct an information risk assessment of your scope of regulatory compliance and use the output of the assessment to make informed decisions with regards to the activities and elements that will be included in your information security program. The output of the information risk assessment should include:

- A clear understanding of the environment being assessed and a definition of the scope of GLBA. The scope of GLBA concerning the GLBA Safeguards Rule should include all the people, process, and technology involved in the handling of NPPI about consumers, including:
 - o **Business services** that require the processing of NPPI about consumers to help deliver a service or product
 - o **People** that handle NPPI directly or indirectly, including external suppliers and third parties
 - o **Processes** that support the delivery of the financial services
 - o **Technology or information systems** that handle NPPI and enable the delivery of financial services
- A list of threats relevant to the scope, the degree to which the information and information systems within the scope are vulnerable to the identified threats, the associated business impacts if those threats manifest, and the technical, administrative, and physical controls that could reduce the likelihood of threats manifesting.
- A list of prioritized residual risk profiles for each of the identified threats in terms of the likelihood of the threat initiating a threat event and exploiting a vulnerability and the threat's effectiveness in exploiting a vulnerability. The residual risk profiles should take into consideration the implementation of current or planned administrative, technical, and physical controls.
- Risk treatment plans to reduce the prioritized risks to a level that is within the organization's risk tolerance by implementing a combination of avoidance, mitigating, and transference activities. Risks that are within the organization's risk tolerance can then be accepted by leadership and regularly monitored to detect any material changes that could increase the risk's severity.

Step 2: Develop a Written, risk-driven Information Security Program

The output of Step 1 should give your organization a solid starting point to begin defining the administrative, physical, and technical safeguards, in terms of people, process, and technology, that will be required to maintain the list of prioritized residual risk profiles within acceptable levels.

The information security program should be based on a proven industry framework. By definition, a framework is a *“basic structure underlying a system, concept, or text”*. Therefore, an information security framework is a basic structure underlying the activities that will be performed to manage information risks within the organization’s risk appetite while improving the organization’s ability to prevent or otherwise detect and respond to attacks.

Generally speaking, a framework should contain an array of activities and desired outcomes for managing information risks and should cover all the information security domains applicable to your organization. Further to that, the framework should also consider information security requirements that your organization must adhere to due to legal or compliance mandates.

The information security framework will be underpinned by people, process, and technology elements, including:

Process:

- Information security policies or statements of management’s intent with regards to protecting information assets.
- Information security processes, procedures, practices, and technical standards that cover the technical, physical, and administrative controls required to implement organizational security policies.

People:

- An individual or group of individuals responsible for managing and measuring the performance of the information security program.
- An individual or group of individuals responsible for implementing the requirements outlined in the security practices and standards, and for effecting defined processes and procedures.
- Individuals responsible for adhering to information security policy requirements for handling business information or using organizational information resources.

Technology:

- The information systems, devices, applications, and networks needed to enforce technical controls to meet the policy objectives.

There are several frameworks that you can choose from as a starting point to develop your own. Examples of popular information security frameworks include NIST Cybersecurity Framework (SP 800-53), Center for Internet Security Critical Security Controls (CIS), Payment Card Industry Data Security Standard (PCI DSS), or ISO 27001. You should consider using a combination of existing frameworks to develop one that is specifically tailored to your organization’s realities and meets the long-term needs of your business, including your regulatory obligations.



The GLBA Safeguards Rule Information Security Framework

The GLBA Safeguards Rule framework of 2003 does not prescribe the elements that must be included in the information security program. It only requires financial institutions to design and implement technical, physical, and administrative controls to manage identified risks, and it provides additional guidance concerning information risk management in the following categories:

- Employee training and management
- Information systems, software, and networks and information processing, storage, transmission, and disposal
- Security incident detection, prevention, and response and other system failures

The proposed changes to the GLBA Safeguards Rule seek to provide more prescriptive guidance with regards to the contents that financial institutions must include in their information security programs. Most of the proposed changes to the GLBA Safeguards Rules are already covered by popular information security frameworks, such as the ones mentioned earlier. Therefore, if you are already following NIST, CIS, or ISO, you are probably well underway to complying with any new changes that may be added to the GLBA Safeguards Rule in the future.

Step 3: Establish an External Supplier Risk Management Capability

Organizations across all industry sectors partner with external suppliers, vendors, and providers of services across the globe to help execute key strategic objectives and goals. In doing so, organizations may need to entrust sensitive business and/or regulated information to third parties and/or grant third-party access to sensitive organizational information systems to achieve service agreements, thus extending their operating environment and information risk assessment scope.

Organizations that do not have a standardized methodology to consistently manage and monitor information risks as part of a procurement or supply chain process could be introducing unwanted risks that could potentially compromise the confidentiality, integrity, privacy, or availability of sensitive business or regulated information.

With regards to the GLBA Safeguards Rule, the FTC requires financial institutions to establish an external supplier risk management capability designed to identify supply chain risks and ensure that external suppliers or service providers are contractually bound to implement and maintain reasonable and suitable safeguards to protect NPPI about consumers in their custody.

To comply with this requirement, you should develop and implement an external supplier risk management capability that is integrated into your procurement or supply chain processes and is supported by:

1. A process for managing information risks associated with external suppliers that handle NPPI (and any other business information) on behalf of your organization. The process should cover:
 - o Identifying the types of NPPI that may be shared with the supplier as well as the types of access that the supplier may need to your organizational information systems.
 - o Defining the security requirements that suppliers must comply with and incorporate those into formal contract agreements.
2. Formal contracts that include:
 - o Information security requirements for suppliers.
 - o Flow-down clauses with regards to sub-contractors and the protection of NPPI.
 - o The right to audit and perform assurance activities to validate that the supplier is meeting your company's requirements.
 - o The right to re-negotiate contractual terms and conditions during the relationship as a result of changes in the supplier's security posture.
3. A process to continuously monitor the security performance of suppliers and re-evaluate their security arrangements before re-negotiating contracts

Step 4: Monitor the Performance of Your Information Security Program


The cyber-threat landscape is constantly changing, with new cyberattack tactics and techniques discovered almost daily. Therefore, your information security program must be continuously evaluated to ensure that the long-term needs of your business are met, that information security investments (in terms of people, process, and technology) yield the desired returns, and that information security risks are managed within your organization's risk appetite.

The GLBA Safeguards Rule requires financial institutions to evaluate and adjust the information security program as a result of testing or when material changes to the business, cyber-threat landscape, or other circumstances impact the effectiveness of existing technical, administrative, or physical safeguards.

To comply with this requirement, you should establish a performance management process designed to evaluate the maturity and performance of your information security program based on your prioritized residual risk profiles, making adjustments as needed to maintain the desired maturity and performance level.

Defining and tracking key performance indicators (KPIs) and key risk indicators (KRIs) are common ways to provide a holistic view of the state of the information security program, allowing leadership to make data-driven decisions. KPIs are measurements that organizations use to determine how well their information security arrangements are performing against strategic goals or objectives while KRIs are metrics designed to measure risks, risk trends, and whether risks are within or above the organization's risk tolerance level. By measuring, tracking, and reporting on the right information security KRIs and KPIs, your organizations will be able to adjust the activities of your information security program and make future investments in security using relevant and accurate data points.





Another way to measure the performance and maturity of your information security program is through information security assurance activities designed to test the effectiveness of administrative, physical, and technical security controls, processes, and procedures. Regular penetration tests, internal and external security audits against your security policies, practices, and procedures, and controls effectiveness testing are some examples of assurance activities that can provide an overview of how well your information security program is performing.

Conclusion

To comply with the GLBA Safeguards Rule, financial institutions are required to protect the security, privacy, confidentiality, and integrity of NPPI through the implementation of technical, physical, and administrative controls. To this end, financial institutions are required to develop, implement, and maintain a written information security program that is driven by reasonably foreseeable internal and external information risks, appoint an individual or group of individuals responsible for managing the information security program and its activities, establish an information risk management capability to identify, analyze, evaluate, treat, and monitor internal and external risks, designing and implementing adequate controls to manage identified information risks to acceptable levels, and measure the performance and maturity of the information security program.

For information security investments to deliver on their promises, information security practitioners should develop information security programs that are driven by business requirements and designed to enable the achievement of business goals and objectives. Using a top-down approach where business, legal, and compliance requirements are identified at the onset and used as inputs to identify information security risks and develop information security requirements to address those risks will ensure that your information security program can meet the long-term and wider needs of the business while also addressing legal and compliance mandates.

ABOUT LEPIDE

Lepide are the fastest growing provider of data-centric audit and protection solutions to enterprises all over the world. The award-winning Lepide Data Security Platform enables you to put your data at the heart of your security strategy; mitigating the risks of data breaches and helping to meet compliance requirements.

Protecting the Data of Thousands of Organizations Worldwide



Western Connecticut
Medical Group

HOGGE · FENTON



FIRSTLEGAL



GE Healthcare

FUJITSU

NHS

Deloitte.

