



GLBA Assessment 2022 Plan

March 2022

[Max Tumarinson](#)

Approach

Residual Risk (Per 2021 GLBA)	No Change (Low Risk Impact)	Non-material Change (Moderate Risk Impact)	Material Change (High Risk Impact)
Low	<ul style="list-style-type: none"> • Business Attestation • No Test 	<ul style="list-style-type: none"> • Walk-through • No Test 	<ul style="list-style-type: none"> • Walk-through • Full Control test
Moderate	<ul style="list-style-type: none"> • Business Attestation • No Test 	<ul style="list-style-type: none"> • Walk-through • No test 	<ul style="list-style-type: none"> • Walk-through • Full Control test
High / Very High	<ul style="list-style-type: none"> • Walk-through • Full Control test 	<ul style="list-style-type: none"> • Walk-through • Full Control test 	<ul style="list-style-type: none"> • Walk-through • Full Control test

- **GLBA approach:**

- Business Attestation: business confirmation in writing that there has been no material change since GLBA 2021.
- Full Control Test: obtain new or leverage IA artifacts to test controls.

- **On change level assessment:**

- Material – Any changes related to design architecture, or technology re-platforming of in-scope Apple Bank Applications, Processes and/or IT Infrastructure Components.
- Non-Material – No Material changes to in-scope Apple Bank Applications, Processes and/or IT Infrastructure Components.

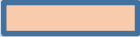









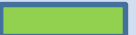




GLBA Execution Plan

Line of Business	Business Department	# of Assessments in 2021	Residual Risk 2021	Anticipated Change in 2022	Proposed GLBA Approach in 2022
Finance & Treasury	Accounting	3	Moderate	Material change	WT (Q4) FCT (Q4)
	Loan Servicing	1	Low	Material change	WT (Q4) FCT (Q4)
Consumer Banking	Digital Banking	6	Moderate	Material change	WT (Q4) FCT (Q4)
	Branch Administration	12	Moderate	Material change	WT (Q4) FCT (Q4)
	Branch Operations	5	Low	Material change	WT (Q4) FCT (Q4)
	Depositor Services	2	Moderate	Material change	WT (Q4) FCT (Q4)
	Consumer Bank Risk & Analytics	1	Moderate	Material change	WT (Q4) FCT (Q4)
	Marketing	1	Low	No change	Attest (Q3) No Test
Commercial Mortgage	Commercial Mortgage Lending	2	Low	No change	Attest (Q3) No Test

GLBA Execution Plan, Continued

Line of Business	Business Department	# of Assessments in 2021	Residual Risk 2021	Anticipated Change in 2022	Proposed GLBA Approach in 2022
Legal and Compliance	Financial Crimes Compliance	4	Low	Material change	WT (Q4) FCT (Q4)
	Legal and Compliance	1	Low	No change	Attest (Q3) No Test
Risk Management	Enterprise Risk Management	1	Low	No change	Attest (Q3) No Test
	Information Security	2	Low	No change	Attest (Q3) No Test
Internal Audit	Internal Audit	1	Low	No change	Attest (Q3) No Test
Information Technology	IT Operations	9	Low	Material change	WT (Q4) FCT (Q4)
	Technology - Data Warehouse	2	Low	Material change	WT (Q4) FCT (Q4)
	IT Infrastructure	15	Moderate	Material change	WT (Q4) FCT (Q4)

Schedule (Illustration)

Department	2022 Q1	2022 Q2	2022 Q3	2022 Q4	2023 Q1
1. Finance & Treasury				 	
2. Consumer Banking				 	
3. Commercial Mortgage					
4. Legal and Compliance				 	
5. Risk Management					
6. Internal Audit					
7. Information Technology				 	

 Attest sunset applications due to Core Conversion
  Attest
  Walk through
  Full control testing*

GLBA Compliance Requirements



Published On - [November 20, 2018](#)
[SCA Blog](#)



The Gramm-Leach-Bliley Act which is also known as the Financial Modernization ACT OF 1999, is a United States federal law that requires all financial institutions to ensure the privacy and security of customer (non-public) information. The Act consists of three sections.

1. **The Privacy Rule** that regulates the gathering and disclosure of private information.
2. **The Safeguards Rule** which specifies that financial institutions must implement safety programs to safeguard such information. This safeguard also applies to ATM operators and companies like credit reporting agencies that collect private information of individuals from financial institutions.
3. **The Pretexting Provisions** that prohibits the practice of obtaining private information and using it under false pretenses.

Who is covered by this Act?

The term 'financial institution' includes many organizations that describe themselves as financial institutions. These institutions include banks, credit unions, payday lenders, mortgage brokers, personal property or real estate appraisers, non-bank lenders among others. If your business deals with loans, the collection of debts, and financial advice, the GLBA applies to you as a financial institution. The law applies to all financial institutions regardless of the size. The Federal Trade Commission (FTC), as well as other government agencies, order financial institutions to implement regulations to meet the GLBA compliance requirements.

What are the GLBA Compliance Requirements?

As part of your GLBA compliance requirement, you are required to meet the three sections of the Act. These sections include The Financial Rule, The Safeguards Rule, and The Pretexting Provisions.

- **The Privacy Rule** is the first piece in your GLBA compliance requirements. It mandates that you provide proper notices of your privacy policies and practices to the individuals who are using your products or services. If an institution intends to disclose a client's private information, it must provide the client with a privacy notice. This notice offers the clients the choice to opt in or out if they choose not to share their personal data with third parties.
- **The Safeguards Rule** requires financial institutions to keep customer information secure. They are also required to ensure that affiliates or 3rd party service providers also take steps to secure customer information. Often mentioned together with information and cybersecurity the Safeguards Rule requires you to perform a comprehensive risk assessment and design, implement and maintain a detailed information [security](#) program to protect customers' private information in all areas of operation.
- **The Pretexting Provisions** section also involves cybersecurity. To comply with this rule, a written plan must be developed for monitoring account activities as well as educating your employees to recognize social engineering and phishing cons.

According to the Federal Trade Commission, the GLBA requirements are made flexible to enable every institution to implement an information security plan that is reasonable and makes sense with the scope and the activities of the company. Enforcement of the GLBA is performed through the member agencies of the Federal Financial Institutions Examination Council (FFIEC) which include the Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), National Credit Union Association (NCUA), Office of the Comptroller of the Currency (OCC) and the Consumer Financial Protection Bureau (CFPB). GLBA also requires an incident response and disaster recovery plans to prepare for and respond to beaches and natural and man-made disasters. Maintaining GLBA compliance is significant to financial institutions as it helps them secure and defend their network while reducing reputation, regulatory and legal risks that can be both expensive and detrimental to continued operations.

Contact SCA Today to Learn More About GLBA Compliance Requirements

Security [Compliance](#) Associates (SCA) has more than 13 years of practice in delivering topnotch [financial security compliance](#), Assessment, and Advisory services to financial institutions throughout the United States. Our assessments include a thorough review of your existing information security posture; the people, process and technology that may compromise sensitive information. SCA employs credentialed analysts and compliance professionals with decades of combined information security experience and will tailor an assessment program unique to your institution's needs, size and culture. Contact SCA today to schedule a no-cost consultation.