Gramm Leach Bliley Act
Data Governance Checklist

Status	GLBC Element		Comment
	Published Privacy Policy and/or FERPA annual notice		
	Process to ensure notice of privacy practices		
	Process to ensure notice when data is shared		
	Annual review of privacy policies		
	Designated Qualified Individual (QI) to oversee information security program		
	QI written report to governing body (at least annually) *		
	Written risk assessment (at least annually)		
		Employee training and management	
		Information systems: network and software design, information processing, storage, transmission, and disposal	
		Detecting, preventing, and responding to attacks, intrusions, or other systems failures	
	Documented safeguard for each risk identified		
		Review of access control standards	
		Full data inventory including data classification	
		Encrypt customer information at rest and in transit	
		Evaluation of application security for in-house and hosted/vendor solutions	
		Multi-factor authentication for all who access customer information	
		Process for secure disposition of customer information	
		Change management process to ensure the ongoing security of information systems and network	
		Logging of authorized user activity including access to customer information	
		Procedures and controls to monitor when sensitive data is accessed	
		Procedures and controls to detect unauthorized access to customer information	
	Regularly monitor and test established safeguards		
		Annual penetration testing	
		Vulnerability assessments, including system-wide scans every 6 months	
		Vulnerability assessment after a material change to business operations and/or identified risk	
	Information Security Program policies and procedures		

Gramm Leach Bliley Act

Data Governance Checklist

Status	GLBC Element		Comment
		Regular security awareness training of all staff who access customer information	
		Specialized training for employees, affiliates, or service providers that have hands-on responsibility for executing information security program	
		Monitor for emerging threats and effective countermeasures.	
		Prevention of unauthorized disclosure of or access to customer financial information	
	Ensure all contracts with service providers specify security expectations and safeguards and include a process to monitor the security practices of the provider		
	Regularly evaluate information security program to account for change		
	Written incident response plan *		
	Controls in place to prevent the unauthorized disclosure of customer financial information		
	Controls in place to detect and mitigate unauthorized access to personal, non-public information		
	Periodic risk assessment of covered accounts, including (1) methods used to open accounts; (2) methods used to access accounts; and (3) previous experiences with identity theft.		
	Written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft		
		Approval from and involvement of the board of directors	
		Staff training	
		Oversight of service providers	

* Required only for institutions maintaining information on over 5,000 consumers

References

Appendix A to Part 681. (2023, June 15). Retrieved June 18, 2023, from National Archives Code of Federal Regulations: ecfr.gov/current/title-16/chapter-I/subchapter-F/part-681/appendix-Appendix%20A%20to%20Part%20681

Cornell Law School. (n.d.). *15 U.S. Code § 6825 - Agency guidance*. Retrieved May 2023, from https://www.law.cornell.edu/uscode/text/15/6825

Federal Student Aid. (2023, 02 09). Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements. *Electronic Announcement ID: General-23-09*.

Federal Trade Commission. (2022, May). FTC Safeguards Rule: What Your Business Needs to Know. Retrieved May 10, 2023, from https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

Title 16 / Chapter I / Subchapter F / Part 681 / § 681.1. (2023, June 5). Retrieved June 18, 2023, from National Archives Code of Federal Regulations: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-F/part-681/section-681.1#p-681.1(c)