SmartSuite

Framework / Financial Services Regulation / Global Privacy Regulations

GLBA Safeguards Rule (16 CFR Part 314)

The GLBA Safeguards Rule requires financial institutions to implement security programs to protect consumer financial information.

What it is

The GLBA Safeguards Rule is a federal data protection regulation that requires financial institutions to implement security controls for safeguarding customer information and ensuring compliance with privacy requirements. Its primary purpose is to protect consumer financial data against unauthorized access, disclosure, and misuse.

Issued by the Federal Trade Commission (FTC) under the Gramm-Leach-Bliley Act (GLBA) and codified at 16 CFR Part 314, the Safeguards Rule applies to a wide range of financial institutions including banks, mortgage lenders, and insurance companies. The regulation mandates comprehensive risk assessments, development and implementation of security programs, and ongoing oversight of service providers, focusing on risk management, data security, and privacy governance.

At a glance

PUBLISHER Electronic Code of Federal Regulations (eCFR)	TYPE Regulation	VERSION GLBA Safeguards Rule (16 CFR Part 314 — 2023 Amendments)
EFFECTIVE May 23, 2003	DOMAIN Financial Services Regulation	FAMILY Global Privacy Regulations
REGION United States	INDUSTRY Financial Services	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

Why it matters

- **Strengthen data protection practices** Reduce the risk of unauthorized access and misuse by establishing robust safeguards for sensitive consumer financial data.
- **Improve cybersecurity governance** Promote accountability and continuous risk assessment through required information security programs and regular management oversight.
- **Enhance regulatory alignment** Support compliance with federal privacy laws and demonstrate diligence to regulators, clients, and business partners.
- **Increase audit readiness** Facilitate easier documentation and validation of security practices to streamline responses during regulatory audits and examinations.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports GLBA Safeguards Rule (16 CFR Part 314)

Safeguards Program Requirement Library

Organize required safeguards with owners, scope, and implementation evidence.

Risk Assessments and Treatment Plans

Run periodic risk assessments and track mitigation actions with approvals.

Access, Encryption, and Monitoring Evidence

Centralize proof for key safeguards tied to customer information protection.

Service Provider Oversight

Manage vendor due diligence, contract requirements, and periodic provider reviews.

Incident Response and Reporting Workflow

Track security events, escalation decisions, and notification readiness.

Audit-Ready Reporting

Report safeguard status, open gaps, and evidence coverage for exams and audits.

Common framework mappings

CIS Controls v8.1 | EU DORA | FFIEC CAT | ISO 27001:2022 | ISO 27701 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

GLBA Safeguards Rule Overview

Describes the key requirements and implementation of the GLBA Safeguards Rule.

ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

FTC Business Guidance on Security

Provides guidance on implementing security practices in line with FTC regulations.

ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

FTC Guidance on Information Security Programs

Outlines how to create and maintain information security programs under the GLBA.

ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

Frequently asked questions

What is the GLBA Safeguards Rule used for?

The GLBA Safeguards Rule is designed to protect consumer financial information held by financial institutions from unauthorized access, disclosure, or misuse. It requires firms to develop, implement, and maintain a comprehensive information security program based on risk management principles.

Is compliance with the GLBA Safeguards Rule mandatory?

Yes, compliance with the GLBA Safeguards Rule is mandatory for all covered financial institutions as defined by the Gramm-Leach-Bliley Act and enforced by the Federal Trade Commission (FTC). Non-compliance may result in regulatory penalties and enforcement actions.

Which organizations fall under the scope of the GLBA Safeguards Rule?

The Safeguards Rule applies to a broad range of financial institutions, including banks, credit unions, mortgage lenders, insurance companies, and nonbank entities engaged in financial activities. Service providers to these organizations may also be subject to certain security requirements.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are the key requirements of the GLBA Safeguards Rule?

Key requirements include conducting regular risk assessments, designing and implementing an information security program with administrative, technical, and physical safeguards, monitoring vendors and service providers, and ensuring ongoing employee training. Documentation and program oversight by senior management or the board are also essential.

How is a GLBA-compliant information security program implemented?

Implementation involves first conducting a risk assessment to identify threats to customer information. Organizations must then establish and regularly update written policies, select suitable controls, conduct employee training, and put in place mechanisms to monitor and test safeguard effectiveness.

How does the GLBA Safeguards Rule align with other security frameworks?

The GLBA Safeguards Rule's risk-based approach aligns with widely used frameworks such as NIST Cybersecurity Framework and ISO 27001. Organizations often map GLBA controls to these standards to leverage existing governance, risk, and compliance efforts for more effective management.

What are the ongoing compliance and maintenance requirements?

Organizations must continuously monitor and test their information security controls, review and update risk assessments, provide regular staff training, and oversee third-party service providers. Incident response processes and management reporting must be maintained to show compliance during audits or examinations.

How would SmartSuite support GLBA Safeguards Rule compliance?

SmartSuite helps organizations manage GLBA Safeguards Rule compliance by centralizing risk tracking, mapping controls to specific regulatory requirements, and streamlining evidence collection for audits. The platform offers dashboards for monitoring control effectiveness, facilitates remediation workflows, and supports audit readiness with robust reporting capabilities.

License included / downloadable: Yes The GLBA Safeguards Rule is a U.S. federal regulation and is publicly available through official FTC and U.S. government publications.

Full framework page and mappings: smartsuite.com/frameworks/glba-safeguards-rule-gramm-leach-bliley-act-16-cfr-part-314