CYERA

Securing Nonpublic Financial Information

# How Cyera Supports GLBA Compliance

# Introduction

## About the Gramm-Leach-Bliley Act

Passed in 1999, the Financial Services Modernization Act - aka Gramm-Leach-Bliley (GLBA) - established privacy protections for customers of financial institutions and consumers of financial services.

The GLBA's privacy protections are found in its Privacy Rule and its Safeguards Rule. The Privacy Rule directs financial institutions to provide notice to its customers (and some consumers) of the types of nonpublic financial information (NPI) it collects and shares with affiliated or unaffiliated third parties, and in some cases an opportunity to opt out.

The Safeguards Rule directs financial institutions to implement an information security program designed to protect customers' NPI from unauthorized access, disclosure, or alteration. The Safeguards Rule doesn't prescribe a one-size-fits-all approach, but requires financial institutions to develop information security programs commensurate with the size and complexity of their businesses. Nevertheless, it does require some concrete policies and practices - consisting of various administrative, technical, and physical controls - that track the requirements of other cybersecurity frameworks like ISO 27001.

This guide will break down the Safeguards Rule, discussing how to use Cyera's Data Security Platform to address its various administrative and technical controls.

## About Cyera

Cyera is a unified, AI-native data security platform that empowers businesses to discover, classify and protect data. It allows security leaders to manage sensitive data across highly permissive and widely distributed environments with high precision and efficiency.

The platform's agentless, fully automated data discovery provides a comprehensive inventory of sensitive data across structured and unstructured sources, and across IaaS, SaaS, DBaaS and on-premises environments. This capability enables organizations to address critical data challenges like data proliferation and drift. Powered by AI-native classification, Cyera goes beyond traditional methods by also understanding context, intent, and nuance - decoding data down to the DNA level. This deep insight helps uncover ghost data, reveal sensitive data risks, reduce false positives, and mitigate threats like data breaches and ransomware — areas where conventional data loss prevention and data governance tools fall short.

By combining advanced technology with ease of use, and scale from its cloud-delivered backbone, Cyera empowers organizations to confidently secure their data, maintain compliance, and unlock the full potential of their data to drive innovation.

# Administrative Controls

## Roles and Responsibilities

Designate the individual(s) responsible for overseeing, implementing, and enforcing your information security program.

Cyera can help identify data owners and responsibilities through asset discovery and classification.

Cyera also provides real-time insight into your data assets and their security posture, alerting on policy violations, and facilitating remediation. This can be helpful in validating data security controls.

## Risk Assessments

Periodically perform risk assessments to identify the reasonably foreseeable internal and external risks to the confidentiality, integrity, and availability of information and information systems.

Establish criteria for evaluating and categorizing security risks, as well as requirements for how identified risks will be mitigated or accepted.

Cyera's Data Risk Assessment service provides your security officials with a virtual, CISO-led evaluation of your organization's data security posture relative to more than 30 controls derived from frameworks such as ISO 27001 and NIST CSF. The service provides actionable intelligence that can help you immediately shrink your attack surface, gain greater visibility into potential threats, and develop a plan for improving your security posture going forward, including timelines and milestones.

## Testing and Monitoring

Regularly test and monitor the effectiveness of security controls. Update the information security program based on findings.

(In the absence of continuous monitoring, organizations must conduct vulnerability assessments every six months and penetration testing on an annual basis.)

Cyera periodically scans your entire data estate, and can be configured to alert on policy violations or the occurrence of anomalous or suspicious activity.

It also integrates with third party tools, including identity providers and SIEM tools, providing critical context and insights for automated processes like incident response or the remediation of access misconfigurations. Event logs can be leveraged to provide deeper analysis of data risks.

## Awareness and Training

Provide personnel with security awareness training.

Provide information security personnel with updates and training sufficient to address identified risks.

Cyera assists your organization in maintaining data security awareness. When a data issue/alert is generated, Cyera has the ability to send a message via email, Slack, or other channel directly to the data owner, notifying them of the issue and providing instructions and guidance for remediation. In this way, Cyera "democratizes" data security in your organization, giving users beyond the SOC team a sense of direct responsibility for maintaining cyber hygiene.

## Third Party Risk Management

Oversee third party service providers to ensure they are implementing adequate information security safeguards.

Periodically assess third party vendors to ensure they are maintaining adequate information security safeguards.

Cyera offers several tools that support the inventorying of external IT service providers, and can help you ensure those providers are adhering to their information security responsibilities.

First Cyera's AI-native DSPM discovers and classifies data across SaaS, PaaS, IaaS, DBaaS, and on-prem resources, giving you visibility into what sensitive data you have, where it resides, who has access to it, and what they're doing with it.

Next, Cyera's Omni DLP can trace your data through users and applications, giving you a better picture of which applications are handling the largest volumes of data, and which are handling the most sensitive data. These insights can be leveraged to help your security team discover unmanaged "Shadow IT" apps and services.

Finally, Cyera's Identity Access creates a catalog of identities accessing your organization's data, whether internal or external, human or non-human. Together, Omni DLP and Identity Access can be used to verify that external IT service providers are adhering to information security responsibilities such as requiring strong passphrases or multi-factor authentication.

## Incident Response Plan

Establish a written incident response plan to ensure timely and effective response and recovery from information security incidents.
**The plan should include:**

- The goals of the plan
- Internal processes for incident response
- Definition of roles and responsibilities
- Processes for internal and external information sharing
- Requirements for remediation of identified weaknesses
- Processes for documenting and reporting security events and incident response activities
- Processes for evaluating and revising the incident response plan

Cyera's Data Detection and Response (DDR) module performs monitoring, detection, and remediation of data incidents. Cyera generates alerts on policy violations, classifies them by criticality, and can integrate with SIEM tools to support automated remediation workflows.

Cyera further supports incident response by helping to determine the data blast radius from a security incident, including information like which users were impacted and which files were exposed.

Cyera's Data Breach Readiness service can help your organization strengthen its data security posture and incident response capabilities. Cyera will scan your existing data stores, inventory and classify your data, and provide a risk report. Our virtual CISOs will evaluate your incident response capabilities based on a targeted set of controls from major industry frameworks like ISO 27001, NIST CSF, and NIST 800-53, and facilitate tabletop exercises to assess your incident response and crisis management capabilities. Based on these findings, Cyera can deliver a prioritized list of recommendations and a roadmap for improving your data security posture and incident response capabilities, including timelines and milestones.

## Internal Reporting

The individual(s) responsible for implementing your information security program must regularly (at least annually) make a report to the board of directors or other governing body setting out the overall status of the program, and specific material matters relating to risk assessments, vendor assessments, results of testing and monitoring, information about security incidents and responses, and recommendations for continuous improvement of the program.

Cyera's DataPort and Cyera MCP dramatically simplify the process of preparing internal reports.

DataPort is a managed Snowflake data warehouse that uses your Cyera data to build clean, analytics-ready datasets, distilling hundreds of tables and billions of data points into a dozen easily digestible tables. DataPort also allows you to augment your Cyera data with integrated datasets from other security providers like Okta or Crowdstrike, and build customizable dashboards that provide mission-critical insights into your information security program.

Additionally, Cyera MCP lets you create an interface between your preferred AI chatbot (Claude, Cursor AI, etc.) and Cyera DataPort. With simple, natural language prompts, you can now get thorough summaries and analyses of your Cyera data, including answers to questions like "which storage buckets are most at risk and how can I secure them?", or "which users have access to Customer X's financial data?"

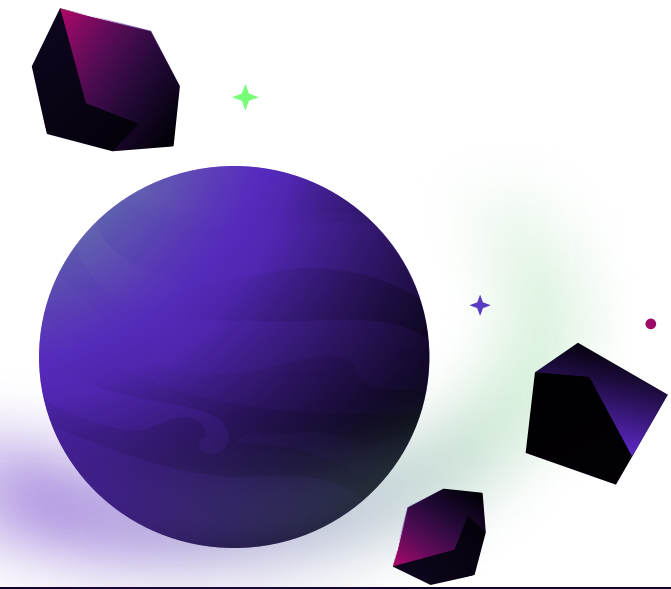
## FTC Notifications

If an information security event impacts the data of at least 500 consumers, you must notify the FTC no later than 30 days after discovery of the event.

**The notification must include:**

- A description of the type of event and information involved in the event.
- The date or date range of the event.
- The number of consumers affected by the event.

Cyera can help your organization rapidly determine whether a particular security event meets the requirements for FTC notification. Cyera generates event logs with timestamps to help you ascertain the date range of the security event and the precise number of consumers affected. Furthermore, Cyera's AI-native classification capabilities provide business context to scanned files, including whether the files pertain to employees, customers, or vendors.



# Technical Controls

## Access Controls

Authenticate and permit access only to authorized users.

Limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information.

Cyera supports this requirement by identifying all users with access to your data, whether they're internal or external to your organization, human or non-human.

Cyera also provides insights on access privileges and usage patterns for each user that can help inform access policies and ensure that they adhere to the principle of least privilege. For example, Cyera can discover the data owner's group or business unit, which can be used in conjunction with other HR or directory tools to detect stale identities, or users who have changed roles within the organization but still retain old access privileges.

## Asset Inventory and Management

Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy.

Cyera discovers and classifies data across your IT ecosystem, including SaaS, PaaS, IaaS, DBaaS, and on-prem environments.

Cyera also catalogs identities with access to your data, whether human or non-human, internal or external.

## Encryption

Encrypt customer data at rest and in transit. If encryption is infeasible for any given data, the designated responsible individual(s) must design compensating controls.

Cyera monitors cryptographic implementations, identifying unencrypted sensitive data at rest and in transit.

Cyera can recommend encryption measures. It can also automatically mask some sensitive data such as credit card numbers or other identifiers.

## Secure Software Development

Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information.

Cyera's DSPM and Omni DLP can be a valuable tool to support secure software and product development.

By providing a clear and thorough picture of your organization's data, Cyera helps you reduce the exposure of sensitive data, enforce access controls and prevent access misconfigurations, and prevent data from being shared outside of development or testing environments. Cyera can even detect when sensitive data has been used in code, and can alert administrators to take remedial action.

## Secure Authentication

Implement multi-factor authentication, or reasonably equivalent secure access control.

Cyera identifies users with access to your data, whether human or non-human, internal or external. Cyera monitors and validates authentication methods used to access sensitive data, and can also verify whether users are adhering to secure authentication policies such as length requirements for passphrases or the use of multi-factor authentication.

## Secure Data Disposal

Develop a data retention and disposal policy. Dispose of all customer data no more than two years after the last date the information was used in connection with providing goods or services to the customer.

Organizations can retain customer data beyond the two year limit only when necessary for legitimate business purposes, is required by law, or when disposal is technically infeasible.

Periodically review the data retention and disposal policy to ensure the minimization of customer data.

Data minimization is a key use case for Cyera. With its unparalleled discovery and classification capabilities, Cyera can help your organization identify orphaned backups, unmanaged drives, and under-utilized virtual machines and databases. It can also discover and classify unstructured data that's been retained in violation of organizational data retention policies. Finally, Cyera can detect remnant sensitive data and validate sanitization efforts.

With Cyera in place, many organizations are already saving tens of thousands of dollars per month in reduced data storage costs, while reducing their attack surfaces and demonstrating compliance with minimization requirements.

## Change Management

Adopt procedures for change management.

Cyera identifies baseline configurations for data storage and access settings across cloud environments, monitors changes, and automatically detects deviations from secure configurations. Cyera also analyzes the security implications of configuration changes on sensitive data.

## Activity Logging

Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

Cyera periodically scans your data estate, and generates data event logs and reports to assist with incident analysis. A live event feed provides alerts into misuse of data, data drifting, or the discovery of exposed sensitive data.

Cyera alerts on policy violations, and can be configured to send messages via email, Slack, or other channel to data owners, with instructions for remediation. Cyera also integrates with third-party SIEM tools for automated incident response.