BitLyft
CYBERSECURITY

BitLyft and GLBA Compliance

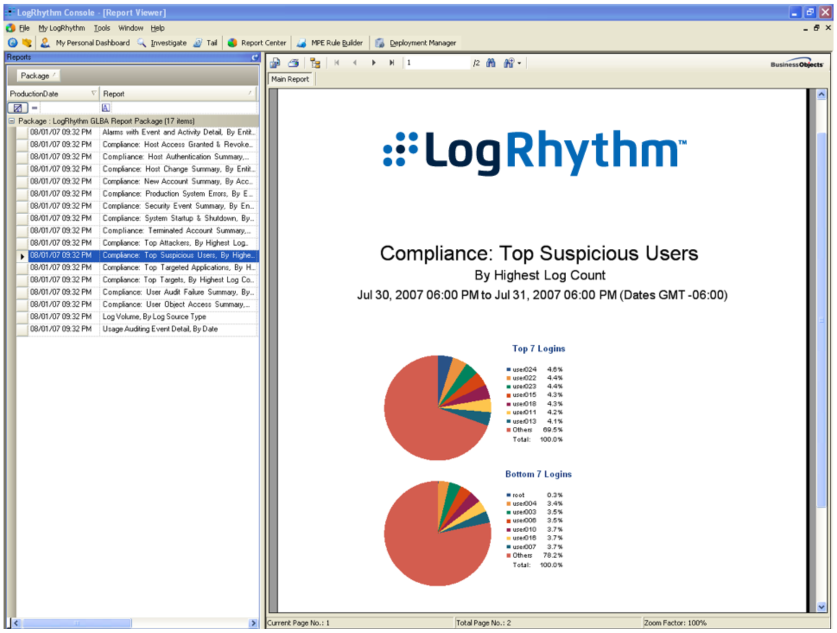
BitLyft and GLBA Compliance

The Gramm-Leach-Bliley Act (GLBA), also known as The Financial Modernization Act of 1999, was enacted to ensure protection over customer's records and information. Authorization to implement this act was given to The Federal Trade Commission (FTC) with an effective date for compliance set on May 23, 2003. GLBA consists of three primary parts; the Financial Privacy Rule, Safeguards Rule, and Pretexting provisions. These rules and provisions make up the requirements for financial institutions to (a) ensure protection of the security and confidentiality of customer's nonpublic personal information (NPI), (b) implement administrative, technical, and physical safeguards, (c) protect against anticipated threats and hazards to information security, and (d) protect against unauthorized access to or use of information. These requirements extend to an institutions business partners as well. Noncompliance can result in penalties that include criminal prosecution, monetary fines and up to 5 years in prison.

To satisfy these legal requirements, financial institutions are required to perform security risk assessments, develop and implement security solutions that effectively detect, prevent, and allow timely incident response, and to perform auditing and monitoring of their security environment. Section 501(b) of the GLBA established the high-level privacy and security requirements that financial institutions must comply with in order to protect customer information.

The collection, management, and analysis of log data is integral to meeting many GLBA requirements. The use of LogRhythm directly meets some requirements and decreases the cost of complying with others. IT environments consist of heterogeneous devices, systems, and applications all reporting log data. Millions of individual log entries can be generated daily if not hourly. The task of organizing this information can be overwhelming in itself. The additional requirements of analyzing and reporting on log data prove manual processes or homegrown solutions inadequate and costly.

LogRhythm can help. Log collection, archive, and recovery is fully automated across the entire IT infrastructure. LogRhythm automatically performs the first level of log analysis. Log data is categorized, identified, and normalized for easy analysis and reporting. LogRhythm's powerful alerting capability automatically identifies the most critical issues and notifies relevant personnel. With the click of a mouse, LogRhythm's pre-configured GLBA report package ensures you meet your reporting requirements.



Package : LogRhythm GLBA Report Package (17 items)

ProductionDate	Report
08/01/07 09:32 PM	Alarms with Event and Activity Detail, By Entit...
08/01/07 09:32 PM	Compliance: Host Access Granted & Revoke...
08/01/07 09:32 PM	Compliance: Host Authentication Summary,...
08/01/07 09:32 PM	Compliance: Host Change Summary, By Entit...
08/01/07 09:32 PM	Compliance: New Account Summary, By Acc...
08/01/07 09:32 PM	Compliance: Production System Errors, By E...
08/01/07 09:32 PM	Compliance: Security Event Summary, By En...
08/01/07 09:32 PM	Compliance: System Startup & Shutdown, By...
08/01/07 09:32 PM	Compliance: Terminated Account Summary,...
08/01/07 09:32 PM	Compliance: Top Attackers, By Highest Log...
08/01/07 09:32 PM	Compliance: Top Suspicious Users, By Highe...
08/01/07 09:32 PM	Compliance: Top Targeted Applications, By H...
08/01/07 09:32 PM	Compliance: Top Targets, By Highest Log Co...
08/01/07 09:32 PM	Compliance: User Audit Failure Summary, By...
08/01/07 09:32 PM	Compliance: User Object Access Summary,...
08/01/07 09:32 PM	Log Volume, By Log Source Type
08/01/07 09:32 PM	Usage Auditing Event Detail, By Date

Compliance: Top Suspicious Users
By Highest Log Count
Jul 30, 2007 06:00 PM to Jul 31, 2007 06:00 PM (Dates GMT -06:00)

Top 7 Logins	
user024	4.6%
user022	4.4%
user023	4.4%
user015	4.3%
user018	4.3%
user011	4.2%
user013	4.1%
Others	69.5%
Total:	100.0%

Bottom 7 Logins	
root	0.3%
user004	3.4%
user003	3.5%
user008	3.5%
user010	3.7%
user016	3.7%
user007	3.7%
Others	78.2%
Total:	100.0%

LogRhythm Report Center Screenshot

GLBA requires financial institutions to implement and perform procedures to identify risks, eliminate or reduce these risks, and to monitor and maintain the implemented processes and procedures to ensure that the identified risks are effectively managed. The Federal Financial Institutions Examination Council (FFIEC), having been tasked with providing guidance and enforcement, has documented the necessary controls for compliance in their "FFIEC Information Security Handbook". The remainder of this paper lists the specific control requirements taken from both the FFIEC Information Security Handbook and associated Tier I and Tier II Examination Procedures. For each control requirement, an explanation of how LogRhythm supports compliance is provided.

Tier 1

Objective 6. Determine the Adequacy of Security Monitory

LogRhythm can collect all relevant log messages that have an impact on security and monitoring responsibilities and alert on violations.

Compliance Requirements	How LogRhythm Supports Compliance
1.6.1 Obtain an understanding of the institution's monitoring plans and activities, including both activity monitoring and condition monitoring. *Activity monitoring consists of host and network data gathering, and analysis.	LogRhythm provides central monitoring of activity and conditions by collecting log data from hosts, applications, network devices, etc. LogRhythm provides real-time event monitoring, alerting, and reporting on specific activity and conditions. **Example Reports:** • System Critical Conditions & Errors • Account Management Activity • System Startup & Shutdown Summary
1.6.2 Identify the organizational unit and personnel responsible for performing the functions of a security response center.	LogRhythm's integrated incident management capabilities support and automate many functions of a security response center. Incidents (alarms) are tracked by status within LogRhythm (i.e., new, open, closed). Activity around the alarm (e.g., notifications, analysis) is recorded in the alarm record. LogRhythm's real-time dashboard provides a heads-up display of incident activity and associated response. LogRhythm reports provide comprehensive reporting on incident activity. **Example Reports:** • Security Event Summary • Alarm & Response Activity
1.6.4 Obtain and evaluate the policies governing security response center functions, including monitoring, classification, escalation, and reporting.	

Objective 7. Evaluate the effectiveness of enterprise-wide security administration

LogRhythm collects and correlates all log data allowing Security Administrators to identify monitor activity and be alerted to specific conditions.

Compliance Requirements	How LogRhythm Supports Compliance
1.7.2 Determine whether management and department heads are adequately trained and sufficiently accountable for the security of their personnel, information, and systems.	LogRhythm's security event management capabilities provide any organization a critical tool in monitoring and responding to the security of information & systems. Having a solution that provides real-time security event monitoring, alerting, and reporting is evidence of management level security diligence and enables audit accountability across the enterprise.
1.7.7 Evaluate the adequacy of automated tools to support secure configuration management, security monitoring, policy monitoring, enforcement, and reporting.	**LogRhythm provides a proven, enterprise class solution for security monitoring. LogRhythm's ability to collect all log data enables reporting on configuration & policy changes. LogRhythm's incident management provides the tracking of applicable enforcement activities.** **Example Reports:** • Host Change Summary • File Integrity Monitoring Activity • Security Event Summary • Alarm & Response Activity

Tier 2

A. Access Rights Administration

LogRhythm collects all access right administration activity for monitoring, reporting, and alerting.

Compliance Requirements		How LogRhythm Supports Compliance
2.A.4	Determine that administrator or root privilege access is appropriately monitored, where appropriate. Management may choose to further categorize types of administrator/root access based upon a risk assessment. Categorizing this type of access can be used to identify and monitor higher-risk administrator and root access requests that should be promptly reported.	LogRhythm collects all account management and account usage activity. The creation of privileged accounts (i.e., administrator, root) or granting of privileged rights is easily and automatically monitored, alerted, and reported on. **Example Reports:** • Account Management Activity • Host Access Granted & Revoked • User Authentication Summary • User Object Access Summary

A. Authentication

LogRhythm can alert or report on all activity performed by privileged or sensitive User Accounts.

Compliance Requirements		How LogRhythm Supports Compliance
2.A.2	Determine whether access to system administrator level is adequately controlled and monitored.	LogRhythm collects all account management usage activity. The creation of privileged accounts (i.e., administrator, root) or granting of privileged rights is easily and automatically monitored, alerted, and reported on. **Example Reports:** • New Account Summary • Host Access Granted & Revoked • User Object Access Summary

B. Network Security

LogRhythm collects logs from network infrastructure and security devices and provides real-time monitoring, alerting, and forensic analysis.

Compliance Requirements		How LogRhythm Supports Compliance
2.B.12	Determine whether logs of security-related events and log analysis activities are sufficient to affix accountability for network activities, as well as support intrusion forensics and IDS. Additionally, determine that adequate clock synchronization takes place.	LogRhythm can collect logs from network devices, IDS/IPS systems, A/V systems, firewalls, and other security devices. LogRhythm provides central analysis and monitoring of intrusion related activity across the IT infrastructure. LogRhythm can correlate activity across user, origin host, impacted host, application and more. LogRhythm can be configured to identify known bad hosts and networks. LogRhythm's Personal Dashboard provides customized real-time monitoring of events and alerts. LogRhythm's Investigator provides deep forensic analysis of intrusion related activity. LogRhythm's integrated knowledge base provides information and references useful in responding to and resolving intrusions. LogRhythm automatically and independently synchronizes audit log time stamps to an absolute time standard (GMT). This ensures the true time of occurrence.

Compliance Requirements		How LogRhythm Supports Compliance
2.B.13	Determine whether logs of security-related events are appropriately secured against unauthorized access, change, and deletion for an adequate time period, and that reporting to those logs is adequately protected. Determine whether logs of security-related events are appropriately secured against unauthorized access, change, and deletion for an adequate time period, and that reporting to those logs is adequately protected.	LogRhythm helps ensure audit trail are protected from unauthorized modification. LogRhythm collects logs immediately after they are generated and stores them in a secure repository. LogRhythm servers utilize access controls at the operating system and application level to ensure that log data cannot be modified or deleted. LogRhythm completely automates the process of retaining your audit trail. LogRhythm creates archive files of all collected log entries. These files are organized in a directory structure by day making it easy to store, backup, and destroy log archives based on your policy.
2.B.17	Determine whether remote access devices and network access points for remote equipment are appropriately controlled. • Remote access is disabled by default, and enabled only by management authorization. • Management authorization is required for each user who accesses sensitive components or data remotely. • Authentication is of appropriate strength (e.g., two-factor for sensitive components). • Modems are authorized, configured, and managed to appropriately mitigate risks. • Appropriate logging and monitoring takes place. • Remote access devices are appropriately secured and controlled by the institution.	LogRhythm collect s network device logs. LogRhythm's analysis & reporting capabilities can used for reviewing network activity to ensure only authorized communications occur. LogRhythm alerts can be used for detecting unauthorized communications. LogRhythm collects remote access activity for VPN, SSH, telnet, etc. LogRhythm reports provide easy and independent review of remote access to information systems. **Example Reports:** • Network Service Summary • Network Connection Summary • Host Remote Access Summary

C. Host Security

LogRhythm collects logs from hosts, and applications running on hosts, to provide real-time monitoring, alerting, and forensic analysis.

Compliance Requirements		How LogRhythm Supports Compliance
2.C.7	Determine whether access to utilities on the host are appropriately restricted and monitored.	LogRhythm can collect audit logs reporting on the access and use of utilities on hosts for monitoring and reporting. Additionally, LogRhythm's file integrity monitoring capability can be used to independently detect access and use of utilities. **Example Reports:** • Host Access Granted & Revoked • User Object Access Summary
2.C.8	Determine whether the host-based IDSs identified as necessary in the risk assessment are properly installed and configured, that alerts go to appropriate individuals using an out-of-band communications mechanism, and that alerts are followed up.	LogRhythm can collect logs from IDS/IPS systems. LogRhythm provides robust alerting and notification capabilities that help ensure alerts are routed to the appropriate individuals. LogRhythm's integrated incident management capabilities provide accountability and reporting on alarm resolution.
2.C.9	Determine whether logs are sufficient to affix accountability for host activities and to support intrusion forensics and IDS and are appropriately secured for a sufficient time period.	LogRhythm helps ensure audit trail are protected from unauthorized modification. LogRhythm collects logs immediately after they are generated and stores them in a secure repository. LogRhythm servers utilize access controls at the operating system and application level to ensure that log data cannot be modified or deleted.

G. Application Security

LogRhythm can be configured to have log data readily available or securely archived for later restoration.

Compliance Requirements		How LogRhythm Supports Compliance
2.G.8	Determine whether appropriate logs are maintained and available to support incident detection and response efforts.	LogRhythm completely automates the process of retaining your audit trail. LogRhythm creates archive files of all collected log entries. These files are organized in a directory structure by day making it easy to store, backup, and destroy log archives based on your policy.

H. Software Development and Acquisition

LogRhythm provides log collection and central analysis for commercial and custom application helping to ensure and automate audit log reviews.

Compliance Requirements		How LogRhythm Supports Compliance
2.H.4	Evaluate whether the software acquired incorporates appropriate security controls, audit trails, and activity logs and that appropriate and timely audit trail and log reviews and alerts can take place.	LogRhythm collects logs from commercial and custom applications. LogRhythm provides central analysis, reporting, and alerting for application logs.

M. Security Monitoring

LogRhythm collects logs from hosts, and applications running on hosts, to provide real-time monitoring, alerting, and forensic analysis.

Compliance Requirements		How LogRhythm Supports Compliance
2.M.1	Identify the monitoring performed to identify non-compliance with institution security policies and potential intrusions. • Review the schematic of the information technology systems for common security monitoring devices. • Review security procedures for report monitoring to identify unauthorized or unusual activities. • Review management's self-assessment and independent testing activities and plans.	LogRhythm can collect logs from IDS/IPS systems, A/V systems, firewalls, and other security devices. LogRhythm provides central analysis and monitoring of intrusion related activity across the IT infrastructure. LogRhythm can correlate activity across user, origin host, impacted host, application and more. LogRhythm can be configured to identify known bad hosts and networks. LogRhythm's Personal Dashboard provides customized real-time monitoring of events and alerts. LogRhythm's Investigator provides deep forensic analysis of intrusion related activity. LogRhythm's integrated knowledge base provides information and references useful in responding to and resolving intrusions. LogRhythm ensures audit trails are protected, retained, and can be easily restored years later. LogRhythm automatically and independently synchronizes audit log time stamps to an absolute time standard (GMT). This ensures the true time of occurrence is known for audit log analysis and reporting.
2.M.5	Determine whether logs of security-related events are sufficient to support security incident detection and response activities, and that logs of application, host, and network activity can be readily correlated.	
2.M.6	Determine whether logs of security-related events are appropriately secured against unauthorized access, change, and deletion for an adequate time period, and that reporting to those logs is adequately protected.	
2.M.7	Determine whether logs are appropriately centralized and normalized, and that controls are in place and functioning to prevent time gaps in logging.	

Compliance Requirements		How LogRhythm Supports Compliance
2.M.8	Determine whether an appropriate process exists to authorize employee access to security monitoring and event management systems and that authentication and authorization controls appropriately limit access to and control the access of authorized individuals.	LogRhythm provides centralized secure access to all log data. LogRhythm leverages application and database level controls to restrict user access to authorized data and functions. LogRhythm includes discretionary access controls for restricting users to a defined subset of the log data collected.
2.M.9	Determine whether appropriate detection capabilities exist related to: • Network related anomalies, including - Blocked outbound traffic - Unusual communications, including communicating hosts, times of day, protocols, and other header-related anomalies - Unusual or malicious packet payloads • Host-related anomalies, including - System resource usage and anomalies - User related anomalies - Operating and tool configuration anomalies - File and data integrity problems - Anti-virus, anti-spyware, and other malware identification alerts - Unauthorized access - Privileged access	LogRhythm can collect logs from hosts, network devices, IDS/IPS systems, A/V systems, firewalls, and other security devices. LogRhythm provides central analysis and monitoring of network and host activity across the IT infrastructure. LogRhythm can correlate activity across user, origin host, impacted host, application and more. LogRhythm can be configured to identify known bad hosts and networks. LogRhythm's alarming capability can be used to independently detect and alert on network and host based anomalies via sophisticated filtering, correlation and threshold violations.